itad

Scoping Study on Fraud Centres:

Ghana, India and Nigeria

Authors: Professor Mark Button, Dr Paul Gilmour, Dr Branislav Hock, Tulika Jain, Dr Sasha Jesperson, Dr Suleman Lazarus, Dr Durgesh Pandey and James Sabia

May 2024

HM Government

Acknowledgements

The team is grateful to the research participants for their openness in discussing the nature of fraud in Ghana, India and Nigeria and the challenges with the response. In addition, Richard Harrison provided input to discussions on recommendations and quality assurance was provided by Philippa Tadele.

Disclaimer

The views expressed in this report are those of the researchers. They do not represent those of Itad, the Home Office or any of the individuals and organisations referred to in the report.

Suggested citation

Itad (2024) Scoping Study on Fraud Centres: Ghana, India and Nigeria. Brighton: Itad.

Copyright

Contents

List of Figures

Acronyms

ABC	Australian Broadcasting Corporation
AI	Artificial Intelligence
AUD	Australian Dollar
BEC	Business Email Compromise
CBI	Central Bureau of Investigation
CEO	Chief Operating Officer
EFCC	Economic and Financial Crime Commission
EOCO	Economic and Organised Crime Office
FBI	Federal Bureau of Investigation
FCDO	Foreign, Commonwealth & Development Office
FIC	Financial Intelligence Centre
GACC	Global Anti-Corruption Consortium
GBP	Great British Pound
HMG	His Majesty's Government
HMRC	His Majesty's Revenue & Customs
HQ	Headquarters
ICT	Information Communication Technology
IRS	Internal Revenue Service
IT	Information Technology
KYC	Know Your Customer
NCA	National Crime Agency
NEET	Not in Education, Employment or Training
NFIB	National Fraud Intelligence Bureau
NGO	Non-Governmental Organisation

NPF	Nigeria Police Force
OCG	Organised Crime Group
ONSA	Office of the National Security Advisor
OTP	One-Time Password
SOC	Serious Organised Crime
UK	United Kingdom
UNODC	United Nations Office on Drugs and Crime
UPI	Universal Payment Interface
USA	United States of America
USD	United States Dollar
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

Executive summary

The 2023 HMG Fraud Strategy indicated that fraud poses a significant threat to the people, prosperity and security of the United Kingdom (UK). It is by far the most common crime and now accounts for over 40% of all offences in England and Wales. Ghana, India and Nigeria have been identified as key jurisdictions of risk for fraud that targets the UK. This research investigated the dynamics of fraud in these three countries and assessed the current response, to identify where the UK can be more active in preventing and tackling fraud.

Methodology

The research began with a desk review of existing literature on fraud, including academic and grey literature as well as media reporting on cases. Interviews were conducted in the UK and internationally with academics, law enforcement and scam fighters. Field research was conducted in Ghana and India, led by national researchers, with interviews being conducted remotely in Nigeria, also led by a national researcher. Semi-structured key informant interviews were conducted with law enforcement agencies, prosecutors, non-governmental organisations, politicians and activists that have been focused on fraud cases, and current and reformed fraudsters.

Dynamics of fraud

Fraud in Nigeria, Ghana and India has evolved on different tracks, with Nigeria and India having a longer history of scams, extending back to the 1980s in the case of Nigeria. In India, phone-based scams from call centres emerged alongside the growth of the legitimate information technology (IT) services industry in the 2000s. Accordingly, the types of scams under way in Nigeria, Ghana and India differ. Common to all three countries is the reliance on social engineering, which uses psychological manipulation to trick individuals into sending money to fraudsters, revealing sensitive information, or taking other actions that jeopardise security. These types of scams take time, as fraudsters need to build trust with their target, but once this trust is established, fraudsters expect high returns. Social engineering is a key element of romance frauds, impersonation scams, blackmail, account takeovers and business email compromise.

These frauds are effective because there are multiple tactics that can be employed by fraudsters, and they are constantly learning and adapting. In addition, the social engineering approach tailors the scam to specific targets. The personal approach also means fraud cannot be detected or averted through electronic means, as targets believe they are forming genuine relationships.

In Ghana and Nigeria, fraudsters operate on a spectrum that extends from individuals working independently to more organised syndicates or groups. In Nigeria, fraud has shifted from an organised activity undertaken in groups to frauds undertaken by lone actors, with a recent shift back to more organised, group activity. In Ghana, less experienced fraudsters operate individually, but there is a growing dominance of groups, with a division of labour. In India, phone-based scams are conducted in call centres, with varying levels of sophistication and scale.

In all three countries, fraudsters tend to be young and educated, and most are male. Economic drivers are the core motivation to become involved in fraud, given the high rates of youth unemployment in Nigeria, Ghana and India. However, in all three countries aspiration also plays

a role, and there is also social value that arises from being a fraudster and being able to displace wealth, particularly in Nigeria and Ghana.

The aim of fraud is to extract money from targets. Various tactics are used to disguise this money and transfer it to fraudsters in the country where the fraud originated. Because direct bank transfers have become too difficult due to increased security measures, alternative strategies are being adopted. These include buying goods that are shipped to the country where the fraud originated, in order to be sold, and the use of cryptocurrency, multiple accounts and hawala[1] networks.

Tackling fraud

As a form of serious organised crime, fraud is addressed by law enforcement. All three countries have legislation in place to address fraud, but the reach of this legislation differs, and challenges arise in putting legislation into practice. Key challenges arise in relation to gathering evidence, particularly on cyber-enabled fraud and identifying frauds and fraudsters. The judicial systems in all three countries also act as barriers to engaging with the available evidence, which undermines prosecutions. Corruption also undermines investigations.

Frauds are not necessarily contained within a country, so international collaboration is required. There is evidence of collaboration between law enforcement agencies in one country and their counterparts in other countries. Increasingly, other actors are also becoming involved, including the private sector and scamfighters – often previous victims of scams, who seek to reveal fraudsters and their tactics.

The response to fraud is also influenced by how it is perceived. Politically, fraud does not receive significant attention unless politicians are directly targeted by fraudsters. Public perceptions of fraud in Nigeria, Ghana and India are mixed, with some supportive of the economic benefits and others viewing it as a crime. Fraudsters also appear to have mixed views on their own activities, as different strategies have been employed to justify their activities.

Conclusions

In all three countries, fraudsters are agile, innovative and adaptive. New technology is adopted, and fraudsters use other mechanisms to enhance their scams, including spirituality, or juju, in Nigeria and Ghana. Innovation and adaptation also occur at a micro level, such as: being able to move to new websites immediately when one is shut down; moving operations to new cities or countries; and reducing the size of scam centres in order to avoid detection. This requires an equally agile response, and although there is evidence to show that law enforcement agencies in all three countries have a good understanding of frauds, prosecutions have not kept pace with scams.

[1] Trust-based networks for moving money without physical money transfers.

1. Introduction

The 2023 HMG Fraud Strategy indicated that fraud poses a significant threat to the people, prosperity and security of the United Kingdom (UK). It is by far the most common crime and now accounts for over 40% of all offences in England and Wales. The Strategy seeks to "Work bilaterally with key countries to strengthen their efforts to tackle fraud, agreeing new actions across government, including law enforcement and Foreign, Commonwealth and Development Office (FCDO) and its networks."[2] The Strategy specifically identifies West Africa and South Asia as priority regions, with the top three jurisdictions of risk being India, Nigeria and Ghana.

In March 2024, the UK hosted a Global Fraud Summit to increase government-to-government cooperation, which to date has been limited. The communiqué issued by the summit recognised that it is the "shared responsibility of governments, law enforcement, industry, regulators, and individuals to combat this rising threat", given the growing sophistication of fraud.[3] However, there are still significant evidence gaps on the nature and dynamics of fraud in key jurisdictions of risk, which affects the development of appropriate responses.

This research sought to address these evidence gaps, conducting scoping and analysis of fraud in the three jurisdictions of risk to understand the methodologies of fraud centres, including: recruitment and targeting; the dynamics of facilitators, including the nature of the actors that establish and manage fraud centres in the three countries; the current response and barriers to investigation; and how fraud is perceived.

Scamming and fraud have a long history in Nigeria. Ellis (2016) and Adogame (2009) have discussed groups of expatriate Nigerian fraudsters, who authored circular letters to dupe individuals with bogus business deals as early as the 1980s.[4] Advance Fee Frauds (or 419 scams as they are known in Nigeria, because of the section of the Nigerian Penal Code that deals with fraud) were once the dominant type, but there is now a wide range of scams. The use of the Internet has made fraud more accessible as a crime and more challenging for law enforcement to track.[5] For example, many fraudsters use a virtual private network (VPN), which disguises their location.[6] These cyber-enabled frauds are undertaken by a new group of fraudsters, known as 'yahoo boys', with the fraud referred to as 'yahoo yahoo'.

Similarly to Nigeria, India has been a major fraud centre for the past two decades, with scams that operate on a global scale, targeting both foreign and Indian nationals. Rather than the cyber-enabled frauds that have become dominant in Nigeria and, more recently, Ghana, 'call centre' or 'phone-based' scams are the predominant methods in India, especially to target

[2] UK government (2023). Fraud Strategy: Stopping Scams and Protecting the Public. Available at: https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf

[3] UK government (2024). 'Policy paper: Global Fraud Summit Communiqué: 11 March 2024'. Available at: https://www.gov.uk/government/publications/communique-from-the-global-fraud-summit/global-fraud-summit-communique-11-march-2024

[4] Ellis, S. (2016). This Present Darkness: A History of Nigerian Organized Crime. London: Hurst; Adogame, A. (2009). The 419 Code as Business Unusual: Youth and the Unfolding of the Advance Fee Fraud Online Discourse. *Asian Journal of Social Science* 37(4): 551–73.

[5] Interview with EFCC, Nigeria.

[6] Interview with NGO, Nigeria.

victims across borders.[7] As in Nigeria and Ghana, these phone scams utilise Internet calling and VPNs to disguise their location.[8]

As cyber-enabled fraud took hold in Nigeria, the phenomenon also increased in Ghana. However, in some ways Ghana can be seen as the junior partner to Nigeria. Nigeria has 'entry-level scams' and more sophisticated scams, but fraudsters in Ghana are predominantly engaged in 'entry-level fraud'. This is a result not of a lack of technological skills in Ghana but of the longer trajectory of fraud in Nigeria, which has resulted in more experience and innovation as compared to in Ghana. In parallel with Nigeria's 'yahoo boys' label, fraudsters in Ghana are referred to as 'Sakawa boys'. Although this term has come to be used to refer to all fraudsters, the term 'Sakawa' specifically refers to the use of spiritualism, or juju, to facilitate fraud[9] (see Section 9.2).

This report provides insight into the dynamics of fraud in the three countries, drawing out the similarities and differences to consider the implications for the relative responses. The report begins by exploring the dynamics of fraud. Section 3 discusses the types of scams under way in each country, whom they target and why they are effective. Section 4 reviews how fraud is organised, analysing how the networks that conduct fraud have evolved and the nature of the actors that establish and manage fraud centres. Section 5 looks more closely at the individuals who are engaged in fraud: the demographics, their motivations and how they are recruited. Section 6 discusses the proceeds of fraud and how they are moved and laundered. The report then turns to the response to fraud within each country in Section 7, exploring the legal situation, law enforcement approaches and collaboration with international partners. Perceptions of fraud are discussed in Section 8: political perceptions, public perceptions, and also how fraudsters themselves rationalise their crimes, because this has implications for the response. Section 9 reviews emerging trends, including improved technology, as well as reliance on spirituality in West Africa to enhance scams. Section 10 draws some conclusions, and Section **Error! Reference source not found.** provides recommendations to tackle fraud in line with the priorities of the Global Fraud Summit. These recommendations will be discussed in a workshop with HMG stakeholders in May 2024 to test and co-create a UK response to fraud.

[7] Interview with scamfighter, India; Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea

[8] Interview with cyber expert, India; interview with fraudster, India; interview with journalist, India; interview with law enforcement, India; Wen, N. J., Carolyn, M., Ang, J., Jingmin, H. and Shuyan, O. (2021). Uncovering the Workings of Credit-for-Sex Scams. Available at: https://www.mha.gov.sg/docs/hta_libraries/publications/07-crime.pdf; Srinivasan, B., Kountouras, A., Miramirkhani, N., Alam, M., Nikiforakis, N., Antonakakis, M. and Ahamad, M. (2018, April). Exposing search and advertisement abuse tactics and infrastructure of technical support scammers. *WWW '18: Proceedings of the 2018 World Wide Web Conference*: 319–28. The use of technology will be further discussed in Section 9.1.

[9] BBC World Service (2023). 'Sakawa Boy reveals how scams work – Love, Janessa, Ep3, BBC World Service and CBC Podcasts'. Available at: https://www.youtube.com/watch?v=N0q1SjLVY0Q

2. Methodology

The research began with a desk review of existing literature on fraud, including academic and grey literature as well as media reporting on cases, and was conducted from December 2023 to January 2024. Significantly more research has been conducted on Nigerian fraud; 117 sources were identified and reviewed, along with 41 sources on fraud in India and 49 on fraud in Ghana. The desk review was used to build up a profile of cases to identify trends and challenges in pursuing cases, as well as prominent gaps to explore during fieldwork. The research identified and analysed 99 cases of convicted fraudsters.

Interviews were conducted in the UK and internationally with academics, law enforcement and scamfighters. Field research was conducted in Ghana and India and was led by national researchers; in the case of Nigeria, interviews were conducted remotely in Nigeria, again led by a national researcher. Semi-structured key informant interviews were conducted with law enforcement agencies, prosecutors, non-governmental organisations (NGOs), politicians and activists that have been focused on fraud cases, and current and reformed fraudsters, who were identified through the networks of the national researchers, purposive sampling and snowball sampling. In total, 43 interviews were conducted – 12 in Ghana, 8 in India, 15 in Nigeria, and 8 with individuals who focused on fraud internationally. Interviews were coded by organisation type to protect the identity of respondents.[10]

Evidence from the interviews and desk review was coded thematically on the basis of the key research questions, with the analysis drawing on the key findings, including similarities and differences between Nigeria, Ghana and India.

[10] Citations are included for each interview, which has created multiples for some references.

3. Scam types

Ghana, India and Nigeria have been identified as key jurisdictions of risk for fraud that targets the UK, but the types of scams under way in each country differ. Common to all three countries is the reliance on social engineering, which uses psychological manipulation to trick individuals into sending money to fraudsters, revealing sensitive information, or taking other actions that jeopardise security.[11] These types of scams take time, as fraudsters need to build trust with their target. A review of more than 500,000 scam emails sent by Nigerian fraudsters found that the use of trust language was linked to higher award claims.[12] Accordingly, there is expectation that once trust has been built, the payoffs will compensate for the time and effort. As one fraudster in Nigeria noted:

> You, the scammer, would become this ideal partner to the client, and from that stage you move on, once solidified, then and from the phase of the relationship, you ask them to buy whatever you want. Since you, the scammer, have filled the gap in the client's life, becoming that ideal woman, he would be taking care of you, so your personal needs, wants, anything you want, you have somebody give you.[13]

Common scams that rely on social engineering include: romance frauds; impersonation scams; the sale of goods and services; account takeovers; and even business email compromise (BEC). These scams vary in the level of sophistication required. Romance frauds, impersonation scams and the sale of goods and services are often viewed as 'entry-level fraud', with fraudsters graduating to more sophisticated scams such as BEC and account takeovers.[14] The entry-level frauds take time to execute but require less technological expertise than account takeovers and BEC. As a result, there are more fraudsters working at this level.

Each of these types of fraud will be discussed, with examples from Ghana, India and Nigeria, before discussing targets and why these scams are so effective.

3.1. Romance frauds

Romance fraud is commonly conducted by fraudsters based in Ghana and Nigeria; it is less common in India, although there are some reported cases that target Indian and UK nationals.[15] In romance frauds, the fraudster adopts a fake online identity and builds up trust and affection with their target before manipulating the victim to send money. This usually starts with small amounts that then steadily increase.[16]

Because the social engineering in these types of scams requires time but less technological expertise than the more sophisticated scams, there are more fraudsters working at this. Romance fraud is a resource-intensive activity, because scammers need to identify potential victims online and tailor their persona to the desires of their target. A review of ten cases of

---

[11] Tookitaki (2023, 4 December). 'Cyber Fraud: Real-Life Examples and Prevention Strategies'. Available at: https://www.tookitaki.com/compliance-hub/cyber-fraud-real-life-examples-and-prevention-strategies

[12] Rich, T. (2018). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal* 31: 208–25.

[13] Interview with ex-fraudster, Nigeria.

[14] Interview with EFCC, Nigeria.

[15] Interview with cyber expert, India; Edwards, M., Suarez-Tangil, G., Peersman, C., Stringhini, G., Rashid, A. and Whitty, M. (2018, May). The geography of online dating fraud. Paper presented at Workshop on Technology and Consumer Protection, San Francisco, California, United States.

[16] Interview with EFCC, Nigeria; interview with fraudster, Nigeria.

romance fraud emphasised the uniqueness of the experience of each victim.[17] This means that fraudsters have invested time into understanding their target.

An estimated 30% of frauds originating from Nigeria are romance frauds, which highlights the diversity of Nigerian frauds.[18] In the case of Ghana, romance fraud is the predominant activity of Ghanaian fraudsters.[19] One interviewee contended that this type of fraud is particularly suited to Ghana, because it needs large numbers of people who are good at telling stories, and it does not rely on sophisticated technology.[20]

Another interviewee noted:

> Fraudsters or scammers in Ghana use deceptive (social engineering) means to obtain money or benefits from unsuspecting victims online. They use persuasive tactics, false promises and misleading information to exploit trust and coerce victims into taking actions that benefit them. They often employ social engineering techniques to exploit human psychology and emotions, such as fear, greed or urgency, to manipulate victims.[21]

Fraudsters deceive victims into believing they are engaged in a trusting relationship, and can then persuade them to send money, provide personal and financial information or purchase items for them; this trust has also been to record explicit videos and images, which are then used to blackmail victims (see Section 3.3).[22]

3.2. Impersonation scams

Social engineering is also used in impersonation scams, in which fraudsters pretend to be legitimate individuals, businesses or organisations in order to deceive victims.[23] This may involve impersonation of government agencies, financial institutions or tech support services to gain victims' trust and extract sensitive information or payments.[24] Other scams involve fraudsters using a fake brand identity to deceive victims into paying for, or providing data in exchange for, the product or service of a recognised brand.[25]

There are cases in Accra, Ghana, in which fraudsters are using fake online listings and social media accounts for legitimate businesses, such as pizza restaurants, to deceive customers.[26] After being offered discounted prices and cheaper delivery rates, victims pay for orders which are never delivered.[27]

---

[17] Aborisade, R. A., Ocheja, A. and Okuneye, B. A. (2023). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology* 3: 100044.

[18] Interview with EFCC, Nigeria.

[19] Interview with an academic, Ghana; interview with an academic, Ghana; interview with law enforcement, Ghana; interview with politician, Ghana; interview with law enforcement, Ghana; interview with fraudster, Ghana; interview with law enforcement, Ghana; Interview with law enforcement, Ghana.

[20] Interview with an academic, Ghana.

[21] Interview with law enforcement, Ghana.

[22] Interview with law enforcement, Ghana.

[23] Interview with law enforcement, Ghana.

[24] Interview with law enforcement, Ghana.

[25] Interview with law enforcement, Ghana.

[26] Korankye, K. A. (2023, 10 November). 'Scammed – Waiting in pain and in vain; The new way online scammers are tricking unsuspecting customers'. Available at: https://www.graphic.com.gh/news/general-news/ghananewsscammed-waiting-in-pain-and-in-vain.html

[27] Ibid.

In Nigeria there are cases of celebrity impersonation scams. These scams take a similar approach to romance frauds, building trust over time, with the victim believing they are forming a genuine relationship with a celebrity.[28] Celebrity impersonation can facilitate requests for the victim to send money or they can evolve into blackmail (see Section 3.3).

In India impersonation is the main tactic, with scammers claiming to provide tech support, often from a big company such as Amazon or Microsoft, or claiming to be from the country's customs, immigration, tax or even drugs enforcement agency.[29] In the 12 months to April 2019, the City of London Police's National Fraud Intelligence Bureau (NFIB) received more than 23,500 complaints related to this form of fraud.[30] A large, English-speaking, computer-savvy youth population, low labour costs, and unsophisticated technology requirements all enabled the emergence and explosion of fraudulent call centres in India.[31]

In tech support scams, scammers from India follow an 'aggressive' or 'passive' approach. Aggressive scams involve generating a pop-up on someone's computer with malware or a virus, and providing an associated number which the victim can call to claim tech support, or cold-calling the victim to inform them of malware. Sometimes these cold calls are automated and are referred to as 'robocalls', which are made automatically by IT-enabled systems. Once the victim engages, the call is transferred to the call centre.[32] The passive approach is where fake tech support websites have phone numbers, which victims call when they 'stumble' upon the site. This number connects them to the call centre.[33] Once the victim is connected, the fraudster uses social engineering methods: they converse with the victim on the phone and convince them that they are legitimate, either gaining access to the person's computer or to their bank details – and draining the account – or making the person buy a worthless piece of software.[34] Fake websites use search results and sponsored ads to reach victims, and they have support domains that aid these websites in manipulating search results.[35] A 2016 Microsoft global survey showed that two out of every three people had been exposed to a tech support scam in the preceding 12 months, of which 86% originated in India.[36]

Another common impersonation tactic is imitating tax and revenue departments, such as the Internal Revenue Service (IRS) in the USA and His Majesty's Revenue & Customs (HMRC) in the

---

[28] Interview with fraudster, Nigeria; interview with fraudster, Nigeria.

[29] Mathai, A. (2022). 'Ever lost money to digital fraudsters? Join the club'. Available at: https://www.theweek.in/theweek/specials/2022/06/24/ever-lost-money-to-digital-fraudsters-join-the-club.html; interview with scamfighter, India.

[30] Dhankar, L. (2023, 2 March). 'Two foreigners held in call centre fraud were planning to flee India, say police'. Available at: https://www.hindustantimes.com/cities/gurugram-news/two-foreigners-held-in-call-centre-fraud-were-planning-to-flee-india-say-police-101677776845652.html

[31] Interview with fraudster, India; Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea; Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0

[32] Lusthaus, J., van Oss, J. and Amann, P. (2023). The Gozi group: A criminal firm in cyberspace? *European Journal of Criminology* 20(5): 1701–18; Liu, X. M. (2021). A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches. *The Coastal Business Journal* 18(1): Article 2.

[33] Interview with fraudster, India; interview with law enforcement, India.

[34] Liu, J., Pun, P., Vadrevu, P. and Perdisci, R. (2023). Understanding, Measuring, and Detecting Modern Technical Support Scams. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*: 18-38.

[35] Srinivasan, B., Kountouras, A., Miramirkhani, N., Alam, M., Nikiforakis, N., Antonakakis, M. and Ahamad, M. (2018, April). Exposing search and advertisement abuse tactics and infrastructure of technical support scammers. *WWW '18: Proceedings of the 2018 World Wide Web Conference*: 319–28.

[36] Economic Times (2021, 4 June). 'How scammers are targeting vulnerable and desperate during India's COVID crisis'. Available at: https://economictimes.indiatimes.com/news/india/how-scammers-are-targeting-the-vulnerable-and-the-desperate-during-indias-covid-crisis/history-of-scams/slideshow/83228982.cms; Khakse, A. and Nambiar, P. (2017). Modern Technology International Crime and Police: An Analysis of Call Centre Crimes in Gujarat. Available at: https://www.academia.edu/38737579/Call_Center_Crimes

UK. These scams use 'phishing' techniques: they send emails or make phone calls that appear to be from reputable sources. The purpose can be to ask for personal information, which is stored in a database for future scams, or to gain financial information and use coercion tactics to convince individuals to pay large amounts of money.[37] As of 2022, American citizens were defrauded of around USD 1 billion from government impersonation and tech support scams.[38]

3.3. Investment scams

Impersonation can also extend to investment fraud. In Ghana:

> Fraudsters impersonate prominent people in society, including members of parliament, ministers or clergy, on social media and use the profiles to promote investment opportunities, including Ponzi schemes with very high returns. Early investors are paid returns using funds from new investors, rather than from legitimate investment returns.[39]

Gold scams are a form of advance fee fraud specific to Ghana because of the country's link to gold mining.[40] Fraudsters claim they have gold and need to transfer it out of the country.[41] Investment fraud is also common in India; for instance, in cryptocurrency fraud, investors are asked to invest increasingly large amounts of money in a 'crypto' scheme and receive initial small payouts to build trust.[42]

Cryptocurrency frauds are increasing in all three countries. There are fake websites created in Nigeria that appear legitimate, but the scam still uses social engineering to convince targets to invest.[43] Cryptocurrency scams have been identified in Nigeria and Ghana,[44] and there are similar scams in India. People start with small investments:

> When you start investing, you see your money increasing, but when you try to withdraw money, you are locked, cannot withdraw. You see a message that you can access in six months due to your type of investment. You keep investing, you start giving more money to withdraw your money.[45]

Nalanda District in Bihar was the hotspot for crypto fraud, but it now comes mostly from Dubai.[46]

3.4. Blackmail and sextortion

Frauds are continually evolving to extract the greatest revenue.[47] Romance frauds and impersonation scams target victims emotionally, and these scams can also transform into

---

[37] Interview with cyber expert, India; interview with fraudster, India; interview with law enforcement, India.

[38] The New Indian Express (2019, October 21). 'UK, India police shut down Kolkata call centres in major online fraud probe'. Available at: https://www.newindianexpress.com/world/2019/Oct/21/uk-india-police-shut-down-kolkata-call-centres-in-major-online-fraud-probe-2050888.html

[39] Interview with law enforcement, Ghana.

[40] Interview with law enforcement, Ghana.

[41] Interview with law enforcement, Ghana.

[42] Interview with cyber expert, India; interview with law enforcement, India; Vaidyanathan, R. (2020, 8 March). 'Confessions of a call-centre scammer'. Available at: https://www.bbc.com/news/stories-51753362

[43] Interview with scamfighter.

[44] Interview with EFCC, Nigeria; interview with EFCC, Nigeria; interview with law enforcement, Ghana.

[45] Interview with cyber expert, India.

[46] Interview with cyber expert, India.

[47] Apantaku, P. O. (2021). Cybercrime: Motivations, Modes, and Emerging Trends, with Nigeria as a Case Study. Doctoral dissertation, University of Portsmouth.

blackmail. Interviews in Nigeria revealed that fraudsters maximise the investment in relationship building by preparing for blackmail. Video calls are recorded, and scammers may threaten to release the video online or post photos shared by the victim. This is particularly the case with celebrity impersonation scams in Nigeria: when victims build up trust that they are engaging with the person they believe them to be, and they believe that this person cares for them, they are willing to share images and sensitive information.[48] One former fraudster stated: "When it comes to blackmailing, they really pay".[49]

Some scams transform into sextortion, with cases being identified in Nigeria and Ghana.[50] For example, if the target has shared private photographs, these can be used for blackmail.[51] It is also becoming a problem in India.[52] Girls are used to lure people; scammers are usually college students.[53] This is further evolving with new technology, as artificial intelligence (AI) can be used to generate fake images to facilitate blackmail (see Section 9.1).

3.5. Scams offering goods and services

Other scams offer goods or services (for a fee) that are never provided. This includes a wide range of services, from job applications to escort services.[54] For example, in the case of fraudulent escort services, clients are told to pay upfront fees for a service that is never delivered.[55] These scams can be targeted anywhere in the world, because there is no need for an actual escort service.

Interviews in Ghana identified challenges with rent fraud, in which the fraudster poses as the owner of an apartment, collects deposits and then disappears.[56] There are also job scams, in which fraudsters impersonate politicians or other high-profile individuals, taking fees from Ghanaians seeking a government job.[57] Similar scams have established services providing assistance to job seekers for a fee, contacting people through social media:[58]

> They will post it on your page that I am just so and so, and if you need any help you can contact me. So you have a lot of people contacting them, and then for them attending you have to pay some initial amount, and then you are given a registration form for you to fill, and then you pay some amount.[59]

Although the fee for these services is small – 300–400 cedi (17-23 GBP) – the scam targets hundreds of victims.

---

[48] Interview with fraudster, Nigeria.
[49] Interview with fraudster, Nigeria.
[50] Interview with scamfighter; interview with HMG.
[51] Interview with scamfighter.
[52] Interview with law enforcement, India; interview with HMG.
[53] Interview with law enforcement, India.
[54] Interview with EFCC, Nigeria; interview with fraudster, Nigeria.
[55] Interview with fraudster, Nigeria.
[56] Interview with law enforcement, Ghana.
[57] Interview with law enforcement, Ghana. Facilitation payments are often paid for government and other high-profile jobs.
[58] Interview with government, Ghana.
[59] Interview with government, Ghana.

In India, schemes include selling cheap (fake) Viagra, offering low-interest loans (and asking for a 'deposit' as proof of income), job placements, and even COVID-19-related scams that targeted people's stimulus packages and offered fake vaccinations.[60]

Advance fee fraud, in which victims are told they are entitled to an inheritance but need to provide bank account details or pay legal fees, also continue in both Ghana and Nigeria.

3.6. Account takeovers

Social engineering is another method used to access the bank accounts of victims. These scams vary in sophistication, as some require fraudsters to navigate banking systems. The aim is to access the account and transfer funds to an alternative account controlled by the fraudster.

Account takeovers are of particular concern to Nigerian law enforcement. Scammers may engage in phishing attacks, send text messages or call, purportedly from a financial institution, to verify information – which, if provided by the target, opens access to bank accounts.[61] Other fraudsters have created X (formerly Twitter) or Facebook accounts that appear to be the customer services departments of banks, and they begin receiving complaints from customers unable to distinguish the fake accounts from genuine accounts.[62] These scams primarily target Nigerian victims, because there are fewer security protocols on Nigerian bank accounts, but the skills being used can also be applied to scams focused on international targets, particularly as Nigerian banks tighten up their security and fraudsters begin looking for other strategies to generate revenue.

There are also more sophisticated account takeovers:

> They check with Telegram, they clone the admin and now go behind to chat to that person on the normal Telegram, the person that had issues with withdrawing. So they go with a different Telegram account to chat to the person on that: 'hello, this is me, I saw that you had issues with depositing.' And they would have, I don't know, got an official link, probably with the help of a bad actor, that is sent to such a person. Upon clicking it I think he would be told to put his key phrase or something.[63]

This tactic is also applied to Telegram groups discussing cryptocurrency transactions.

In Ghana there are tactics to defraud mobile money users.[64] Mobile money is a mobile payments system in which accounts are held by mobile operators and are accessible from subscribers' mobile phones. Scammers use the different mobile platforms, such as MTN Mobile Money and Vodafone Cash, to trick people into sending them money or sharing their mobile money PIN. As part of their operations, these fraudsters pose as service agents, customers, or employees of the

[60] Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0; Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231; Chaganti, R., Bhushan, B., Nayyar, A. and Mourade, A. (2021). Recent Trends in Social Engineering Scams and Case Study of Gift Card Scam. arXiv preprint. arXiv:2110.06487; Office of Public Affairs (2016, 27 October). 'Dozens of Individuals Indicted in Multimillion-Dollar Indian Call Center Scam Targeting U.S. Victims'.

[61] Interview with EFCC, Nigeria.

[62] Interview with EFCC, Nigeria.

[63] Interview with EFCC, Nigeria.

[64] Interview with law enforcement, Ghana; interview with government, Ghana.

mobile money service. They employ various tactics, such as fake promotions, refunds, or emergencies, to persuade the victim to transfer money to their account.[65]

Fraudsters have also deceived Ghanaian victims into providing the one-time password (OTP) sent by their bank to access online banking.[66] In this way, fraudsters avoid the need to hack into the banking system, instead accessing accounts directly. Similar tactics are used to get victims to change their PIN and share it with the fraudster.[67] The use of juju (see Section 9.2 on the rise of spirituality in fraud) is often important in these scams, so that "when they talk to you, their voice should be able to lull you into accepting whatever it was. […] They want to talk to your face and then tell that whenever you get an alert to enter your PIN".[68]

Account takeover is also a tactic used by Indian fraudsters. As mentioned in Section 3.2, call centres impersonate tech support workers, government staff or even surveyors, and gather personal and banking information (including Social Security numbers) or gain remote access to people's computers, and hence to their financial accounts.[69]

3.7. Business email compromise

BEC provides an avenue for large-scale fraud. Also based on social engineering tactics, BEC aims to compromise business email accounts by duping email recipients into clicking on a link, although computer intrusion techniques are also used.[70] The three dominant scams deployed by Nigerian fraudsters are wire transfer attempts, payroll fraud, and compromises that have led to follow-on spam campaigns.[71]

Despite the categorisation of Ghana as engaged in entry-level fraud, there are reports of more sophisticated fraud, and this can be expected to increase. There have been cases of BEC identified in which scammers impersonate legitimate businesses or individuals though email, manipulating recipients into revealing sensitive information, making unauthorised payments, or engaging in other fraudulent activity.[72]

3.8. Targets

The primary targets for fraud are international for Nigerian and Ghanaian fraudsters. Some cite moral reasons – that they do not want to scam their fellow nationals because of the economic situation, or as payback for colonialism (see Section 8.3 for strategies to rationalise fraud). However, the key driver is the potential for larger payouts.

One Ghanaian interviewee estimated that 78%–80% of targets are outside Ghana, mostly in the USA (primary target) and the UK (secondary target).[73] The Ghanaian Financial Intelligence Centre (FIC) records between 400 and 500 cross-border fraud-related cases each year.[74] However,

---

[65] Interview with law enforcement, Ghana.

[66] Interview with law enforcement, Ghana.

[67] Interview with government, Ghana.

[68] Interview with government, Ghana.

[69] Chaganti, R., Bhushan, B., Nayyar, A. and Mourade, A. (2021). Recent Trends in Social Engineering Scams and Case Study of Gift Card Scam. arXiv preprint. arXiv:2110.06487.

[70] Crowdstrike (2018). Intelligence Report: CSIR – 18004: Nigerian Confraternities Emerge as Business Email Compromise Threat. Available at: https://www.crowdstrike.com/wp-content/uploads/2020/03/NigerianReport.pdf

[71] Ibid.

[72] Interview with law enforcement, Ghana.

[73] Interview with politician, Ghana.

[74] Interview with law enforcement, Ghana.

there are frauds that operate domestically, targeting Ghanaian victims. Some social engineering practices target Ghanaians, including impersonation fraud and account takeovers. Similarly, in Nigeria the majority of frauds target internationals, but there is a growing number of domestic frauds, particularly among less experienced fraudsters.

Call centres in India target victims from the USA, the UK, Canada, India and Australia (in this order of preference, as per the FBI's 2022 Internet Crime report).[75] Increasingly, victims from other European countries and places with a high proportion of English speakers, such as South Africa and Singapore, are also being targeted.[76] There are mixed views on whether the Indian diaspora is also targeted. One fraudster interviewed claimed that they avoid taking money from a person of Indian origin, but almost every other source claimed that Indians are a target as well.[77] It is more likely that Indians are targeted by most call centres, with immigration-related issues and the threat of deportation used as tactics to scare victims and extract money. For instance, a centre in Kolkata was calling Indian students whose visas were about to expire with an offer of a job in Australia for AUD 800 (420 GBP).[78] Job placement scams are common and are directed at both people living in the country and diaspora in other countries, such as in the Gulf.[79]

It is important to note that domestic fraud is also a massive industry in India, and law enforcement deals primarily with these cases (see Section 7.2).[80] The tactics used to target domestic victims are even more varied and innovative. Victims are promised returns for minor tasks such as reviewing YouTube videos, or are encouraged to invest in schemes, with small payouts to gain trust.[81] There have been reports of people falsely selling oxygen cylinders (during the pandemic), coaching classes, online discount coupons, and even points on games such as Roblox and PUBG. India's booming digital Universal Payment Interface (UPI), which has experienced widespread adoption over the past five years, is being used to extract money using the duplication of SIM cards (to access OTPs) and manipulating the 'send' and 'request' features to trick people into giving away their money.[82] In this respect India is similar to Nigeria and Ghana, where the large-scale adoption of highly fungible digital money has enabled fraud, because the technologies are relatively new and hence awareness of scam tactics is lower. According to a Microsoft study, out of 16 countries surveyed, India reported the biggest increase

---

[75] The New Indian Express (2019, October 21). 'UK, India police shut down Kolkata call centres in major online fraud probe'. Available at: https://www.newindianexpress.com/world/2019/Oct/21/uk-india-police-shut-down-kolkata-call-centres-in-major-online-fraud-probe-2050888.html

[76] Harley, D., Grooten, M., Burn, S. and Johnston, C. (2012). My PC has 32,539 errors: how telephone support scams really work. Virus Bulletin.

[77] Interview with fraudster, India; Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0; Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea; interview with cyber expert, India; interview with law enforcement, India; Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231; Economic Times (2021, 4 June). 'How scammers are targeting vulnerable and desperate during India's COVID crisis'. Available at: https://economictimes.indiatimes.com/news/india/how-scammers-are-targeting-the-vulnerable-and-the-desperate-during-indias-covid-crisis/history-of-scams/slideshow/83228982.cms

[78] Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea

[79] Economic Times (2021, 4 June). 'How scammers are targeting vulnerable and desperate during India's COVID crisis'. Available at: https://economictimes.indiatimes.com/news/india/how-scammers-are-targeting-the-vulnerable-and-the-desperate-during-indias-covid-crisis/history-of-scams/slideshow/83228982.cms

[80] Interview with law enforcement, India.

[81] Interview with law enforcement, India.

[82] Vaidyanathan, R. (2020, 8 March). 'Confessions of a call-centre scammer'. Available at: https://www.bbc.com/news/stories-51753362; interview with cyber expert, India.

in the number of people losing money through tech support scams, indicating that domestic victims are the biggest target.[83]

3.9. Effectiveness

Fraud is effective because there are multiple tactics that can be employed by fraudsters, and they are constantly learning and adapting. In addition, the social engineering approach tailors the scam to specific targets, which, although resource-intensive, results in higher returns.

A secondary review of trends, patterns and consequences of cybercrime in Nigeria found that fraudsters are intelligent and dynamic individuals who consistently update their tactics; they understand the psychology of potential victims and are able to manipulate those victims' state of mind and ego.[84] The effectiveness of social engineering approaches also relies on many victims being too embarrassed to report their experience.

As in Nigeria, Ghanaian fraudsters are constantly innovating and evolving their tactics to remain one step ahead of law enforcement and security measures.[85] Hacked Facebook and X/Twitter accounts can be bought online, and cadres of young people looking for income are ready to populate these accounts and maintain them as if they are real people.[86] Ghana is particularly well equipped to be a hub for fraud: the country has more phones than people, and it has high youth unemployment and cheap Internet connection.[87] In addition, scripts for different scams can be purchased online. Journalists investigating cyber fraud found "military formats, sick mother scripts, lotto formats, gay sex chat formats, sugar daddy formats and 'trust and love' scripts".[88]

In India, phone scams are able to successfully extract money from individuals by using a number of methods. They are customised to fit the profile of the victim being targeted and can use social engineering to coerce victims. Many scams are 'mixed and matched' based on how the call is going and who the target is.[89] Often they target senior citizens, people who have limited knowledge of technology, and those who may not have friends or family nearby.[90] There have been a reports of a "sucker's list" of people who have been scammed before and are easy targets.[91] Interestingly, data shows that young people aged 18–24 are also likely to get scammed, as they have more of an online presence and public information, making social engineering easier. They may also participate in more risky activities.[92]

---

[83] Khakse, A. and Nambiar, P. (2017). Modern Technology International Crime and Police: An Analysis of Call Centre Crimes in Gujarat. Available at: https://www.academia.edu/38737579/Call_Center_Crimes

[84] Ayub, A. O. and Akor, L. (2022). Trends, Patterns and Consequences of Cybercrime in Nigeria. *Gusau International Journal of Management and Social Sciences* 5(1): 241–62.

[85] Interview with law enforcement, Ghana.

[86] Adebayo, B. (2023, 15 August). 'Sakawa Boys: Meet Ghana's online romance scammers'. Available at: https://www.context.news/digital-rights/sakawa-boys-meet-ghanas-online-romance-scammers

[87] Rubinsztein-Dunlop, S., Robinson, L. and Dredge, S. (2019). 'Meet the scammers: Could this be your online lover?' Available at: https://www.abc.net.au/news/2019-02-11/ghana-meet-the-scammers/10785676

[88] Ibid.

[89] Tzani Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R. and Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. *Journal of Forensic and Investigative Accounting* 12(1): 163–78; Liu, J., Pun, P., Vadrevu, P. and Perdisci, R. (2023). Understanding, Measuring, and Detecting Modern Technical Support Scams. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*: 18–38; interview with scamfighter, India.

[90] Interview with law enforcement, India.

[91] Tzani Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R. and Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. *Journal of Forensic and Investigative Accounting* 12(1): 163–78.

[92] Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231; Khakse, A. and Nambiar, P. (2017). Modern Technology International Crime and Police: An Analysis of Call Centre Crimes in Gujarat. Available at: https://www.academia.edu/38737579/Call_Center_Crimes

Scammers receive training to specialise in sales, deception, extortion and misinformation. They sometimes use a more fear-based, threatening approach, exploiting the facts that people in Western countries fear State entities such as the IRS and tend to comply with authority figures.[93] They also evoke a sense of urgency, applying pressure to make rushed decisions, leading to the victims handing over their money without gathering the necessary information.[94] In the tech support space, the pop-ups often appear when a person is accessing illegal downloads or pornography, in which case they are more scared and compliant.[95] In one example, a gang targeted high-profile victims and told them that child pornographic material had been confiscated at the border, along with their contact information.[96] As mentioned previously, passive tech support scams manipulate search engines and ad networks to get clicks on their fake websites.[97]

Another reason these scams are effective is the speed and agility with which they adapt and evolve, similarly to the way they do in Nigeria and Ghana. The number of COVID-19 scams that emerged during the pandemic is testament to the fact that scammers exploit all opportunities available.[98] An Indian cybercrime expert said, "Awareness is not enough. […] People are getting targeted regardless of their level of education. [The] modus operandi changes every day." The tech support scam industry is a good example. It is almost a decade old and has become more sophisticated over time, relying more on inbound calling – through ads, pop-ups and fake websites – than outbound calling as awareness and security protection have increased.[99] When one scam group develops a new technique for scamming, the idea spreads gradually to other groups. Because customers are not as gullible as before, there is pressure among call centres to come up with new methods.[100]

In all three countries there are multiple scam types under way, and they are frequently evolving in order to avoid detection and suspicion from targets. Despite increased awareness of fraud, particularly from Ghana, India and Nigeria, the use of social engineering continues to be effective in grooming victims for extortion.

---

[93] Tzani Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R. and Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. *Journal of Forensic and Investigative Accounting* 12(1): 163–78; interview with cyber expert, India; interview with fraudster, India; Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0; Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231; interview with law enforcement, India.

[94] Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231; interview with fraudster, India.

[95] Economic Times (2021, 4 June). 'How scammers are targeting vulnerable and desperate during India's COVID crisis'. Available at: https://economictimes.indiatimes.com/news/india/how-scammers-are-targeting-the-vulnerable-and-the-desperate-during-indias-covid-crisis/history-of-scams/slideshow/83228982.cms

[96] Mathai, A. (2022). 'Ever lost money to digital fraudsters? Join the club'. Available at: https://www.theweek.in/theweek/specials/2022/06/24/ever-lost-money-to-digital-fraudsters-join-the-club.html

[97] Economic Times (2021, 4 June). 'How scammers are targeting vulnerable and desperate during India's COVID crisis'. Available at: https://economictimes.indiatimes.com/news/india/how-scammers-are-targeting-the-vulnerable-and-the-desperate-during-indias-covid-crisis/history-of-scams/slideshow/83228982.cms

[98] Chaganti, R., Bhushan, B., Nayyar, A. and Mourade, A. (2021). Recent Trends in Social Engineering Scams and Case Study of Gift Card Scam. arXiv preprint. arXiv:2110.06487.

[99] Srinivasan, B., Kountouras, A., Miramirkhani, N., Alam, M., Nikiforakis, N., Antonakakis, M. and Ahamad, M. (2018, April). Exposing search and advertisement abuse tactics and infrastructure of technical support scammers. *WWW '18: Proceedings of the 2018 World Wide Web Conference*: 319–28; interview with fraudster, India.

[100] Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea; interview with scamfighter.

4. The organisation of fraud

In Ghana and Nigeria, fraudsters operate on a spectrum that extends from individuals working independently to more organised syndicates or groups.[101] In Nigeria, fraud has shifted from an organised activity undertaken in groups to greater involvement of lone actors, with more organised group activity again becoming more prominent. The result is a mixture of individuals, variously sized groups of varying sophistication, and sophisticated organised confraternities. In Ghana, less experienced fraudsters operate individually, but there is a growing dominance of groups, with a division of labour. In India, phone-based scams are conducted in call centres, with varying levels of sophistication and scale. Less is known about the organisation of scams that target Indian victims (such as UPI scams or romance fraud) and whether they are based outside of call centres.

This section analyses the structure of fraud in India, Ghana and Nigeria, focusing on the country level.

4.1. Nigerian fraud actors

There are multiple structures facilitating fraud in Nigeria. These include lone actors that access more established networks for expertise or services, networks with varying levels of hierarchy, and, at the more organised end, confraternities – organised groups that originated in universities and are associated with serious organised crime (SOC).

4.1.1. Lone actors

Early scams originating from Nigeria, involving physical letter-writing, required a large network to facilitate fraud, often based in multiple countries. The role of the Internet and the rise of cyber-enabled fraud have reduced the barriers to entry. Although prospective fraudsters still require means to access a laptop, many fraudsters have started working independently from cafes. Initially cyber fraudsters worked independently, but the percentage of lone actors is now very small, as the value of economies of scale is recognised and more sophistication is required to evade law enforcement:[102]

> When cybercrime started, usually we had more lone actors than organised groups, because all I needed to do then is phish out email addresses, send fictitious emails, your response is, like, prepared for months. Once you respond to the first mail, I send you the second mail. Once you respond, what happens next is okay, you start sending money. Once you start sending money, all that you require from me is just send me the amount and the test questions, then I can give any name, and I can just go to the bank with a forged driver's licence, a forged ID card, and receive the money. But we have passed that stage because of the mechanism that has been put in place by the government to track down.[103]

[101] Interview with fraudster, Nigeria.

[102] Interview with EFCC, Nigeria.

[103] Interview with EFCC, Nigeria.

Some who continue to work alone have a network of support or use social media to share information in loose groups, or they engage in some joint work, but then the proceeds of fraud are divided among the group.[104]

Two lone actors that have been identified in Nigeria include *Adegbayi*, a romance fraudster who created fake profiles on Facebook and who was convicted of defrauding a USA citizen of USD 200,[105] and *Louis*, a crypto fraudster found guilty of impersonating a Brazilian bitcoin trader.[106]

4.1.2. Networks

The more sophisticated the fraud, the more likely it is that it is facilitated by a group. For example, BEC frauds are rarely managed by lone actors. There is evidence of hierarchical structures being formed in Nigeria – often organically. A small group will form, with leaders teaching others how to scam.[107] This then expands into a hierarchy, with new recruits coming in at the bottom, learning the trade, and with revenue flowing up to the group leaders.[108] Aspiring scammers know who the fraudsters are and will approach them, seeking mentorship.[109] This process moves the mentors up in the hierarchy. The leaders of these groups are referred to as 'Egbon Adugbo' – a term which usually refers to a respected male figure such as an older brother. Individual fraudsters can tap into more established groups, paying in to get contacts, leads or tools for scamming.[110] Interviews also identified that training centres are being set up in hotels, targeting people as young as 10–12 years old.[111] Universities have also traditionally been a hub for recruitment, particularly among technology and engineering students.

Groups may be based in an Internet cafe, apartment or hotel, often referred to as 'Hustle Kingdoms'. Networks are usually based upon family, friendship and regional ties and they often lack formal structures, although interviews highlighted common roles within these structures: "There are different areas of specialisation. […] Some people can be the ones that are involved in using your SIM; some people can be the ones that are involved in accessing your accounts".[112]

In addition to the leader, or 'Oga',[113] there is a range of frontline workers within these groups, including:

- allrounders
- victim finders (bombers): those that send out phishing emails, search social media and websites to identify targets
- hackers: those with the technical skills to hack accounts and systems

---

[104] Interview with EFCC, Nigeria; interview with fraudster, Nigeria.

[105] Ogune, M. (2023, 28 June). 'EFCC Secures Conviction of Two Internet Fraudsters in Abuja'. Available at: https://guardian.ng/news/efcc-secures-conviction-of-two-internet-fraudsters-in-abuja/

[106] Ogune, M. (2023, 18 July). 'Court sends four internet fraudsters to prison in Benin City'. Available at: https://guardian.ng/news/court-sends-four-internet-fraudsters-to-prison-in-benin-city/

[107] Interview with EFCC, Nigeria.

[108] Interview with EFCC, Nigeria; interview with NGO, Nigeria.

[109] Interview with NGO, Nigeria.

[110] Interview with fraudster, Nigeria.

[111] Interview with NGO, Nigeria.

[112] Interview with NGO, Nigeria.

[113] 'Oga' is used to refer to the boss in Nigeria; it is drawn from the Igbo word 'ogaranya', which means 'influential senior' or 'boss'.

- catchers/finishers (Guyman): lead the final stage of convincing victims to send money
- scam development: designing and refining scams
- apprentices: those learning how to be a scammer.

There are also other actors who provide specific services. These include: money laundering (see Section 6 for a discussion on the proceeds of fraud), which is usually built upon the diaspora, and includes herders (those who organise the money laundering); money mules, who receive payments from victims; and donkeys, who receive and ship consumer goods purchased with illicit funds, which are then sold to recover the revenue.

Fakermakers are facilitators, who deliver technical services to Ogas, although some also engage in scams. These actors supply a wide range of services, including web design, registration of websites, obtaining hosting space, populating hosting space, maximising the life of fraudulent websites to ensure they appear realistic, sending emails, creating fake social media profiles, creating fake documents, and other related tasks. There are also *auxiliaries* – roles that can be drawn upon to support scamming, such as bank staff, police officers, judges, and insiders within key organisations. These individuals might be involved opportunistically or may have more established relationships with fraud groups. *Priests* have also been implicated, providing spiritual support for scammers through justification and believed impact on victims (juju in Nigeria, Sakawa in Ghana); this is discussed in more detail in Section 9.2.

The organisation into loose networks makes it difficult for law enforcement because fraudsters may not be physically working together in the same location (or country). In many cases, individuals have been arrested but they are suspected of being part of a syndicate. For example, Scales Olatunji was convicted for impersonating a former Norwegian Football Association President to defraud a charity of €64,000 (55,400 GBP); he is suspected of being part of a syndicate, specialising in BEC fraud, that has netted over €500,000 (428,800 GBP).[114]

There have been some successes in identifying wider networks. Two other Nigerians, Samuel and Samson Ogoshi, were arrested for involvement in a global sextortion group and have been extradited to the USA; a third arrest is pending.[115] Ghanaian Maxwell Atugba Abayeta was extradited to the USA for being part of a group conducting BEC fraud and romance frauds against North American companies and individuals; this followed the conviction of seven other members, some of whom were Nigerian.[116]

The Nigerian diaspora in Western Europe and North America also play an important role organising fraud and money laundering, with some evidence of links to confraternities. There have been numerous examples of Nigerians who have recently moved abroad or are second generation immigrants conducting fraud and/or money laundering at low levels and as part of highly organised schemes. There is also evidence of recruitment within the diaspora, including individuals recruited as money mules, but also insiders and technically skilled professionals to

[114] Ogune, M. (2023, 28 June). 'Notorious internet fraudster to spend 235 years imprison for N252million fraud'. Available at: https://guardian.ng/news/notorious-internet-fraudster-to-spend-235-years-imprison-for-n525million-fraud/

[115] Campbell, J. (2023, 14 August). '2 Nigerian men accused of running a global 'sextortion' ring linked to a teen's suicide have been extradited to US, officials say'. Available at: https://edition.cnn.com/2023/08/14/us/michigan-sextortion-ring-nigerian-suspects-extradited/index.html

[116] United States Attorney's Office (2020, 26 August). 'Ghanaian Citizen Extradited in Connection with Prosecution of Africa-Based Cybercrime and Business Email Compromise Conspiracy'. Available at: https://www.justice.gov/usao-wdtn/pr/ghanaian-citizen-extradited-connection-prosecution-africa-based-cybercrime-and-business

help facilitate frauds from the target countries. In the case of Junior Boboye (see box in section 4.1.3), the leaders of the fraud network were predominately Nigerian diaspora.[117]

4.1.3. Confraternities

At the most organised end of the spectrum, there are numerous confraternities in Nigeria that are connected to regions and specific universities. Some of these groups, most notably Black Axe, have been implicated in other types of SOC, including human trafficking, arms trafficking and drug trafficking. The degree of involvement of confraternities in fraud is very difficult to determine, but there are indications of involvement in the direction of fraud in some cases and the facilitation of networks to enable members to find relevant expertise and functions to commit fraud.

Some law enforcement agencies have often assumed that detected fraudsters are working alone or in small groups, but there is growing evidence from some seizures of mobile phones and other evidence from some investigations that there are wider organised international, but hidden networks linked to these cases. Evidence from recent enforcement activities in the Republic of Ireland related to both frauds and money laundering found significant evidence of Black Axe involvement which included standard template recruitment forms for money mules, common terminology (which have been found in investigations in other countries) and messages from seized from mobile phones indicating a command and control structure of several levels, headed by an externally based 'chairman'.[118] In one case, key actors implicated had allegedly been sent from Nigeria to Ireland as an asylum seeker to 'increase revenues' from fraud.[119]

The confraternities, or cults, have a long linkage to scams.[120] In 2015, a fraudster known as the 'king of dating' confessed to his scamming activities during a church service, explaining that he became involved in scamming after joining the Black Axe cult.[121] However, a survey of cult members in the Niger Delta region by the United Nations Office on Drugs and Crime (UNODC) found fraud and scams to be low on the list of criminal activities that cult members were engaged in.[122] On the other hand, internationally there have been many cases that have implicated the Black Axe cult. INTERPOL's 2023 Operation Jackal included a focus on the Black Axe and other West African organised crime groups (OCGs).[123]

Black Axe (which is often linked to the Neo Black Movement) is a sophisticated organisational structure built upon a headquarters (HQ) and delegated zones, which are further subdivided. It has a constitution governing its operations and covering issues such as discipline. Some of the key roles in the organisation which have been identified include HQ, Zonal head (region leader), Ihaza (finance), Eye (intelligence), Crier (public relations), Butcher (security of the group), Priest

---

[117] Sunday World (2023). Faces of Black Axe international fraud gang members after being busted in Ireland. Available at: https://www.sundayworld.com/crime/irish-crime/faces-of-black-axe-international-fraud-gang-members-after-being-busted-in-ireland/a357806436.html and

Irish Independent (2023) Explainer: Who are the Black Axe Gang? Available at: https://www.youtube.com/watch?v=N7TSP3IE2SQ

[118] Interview with law enforcement, Ireland.

[119] Interview with law enforcement, Ireland.

[120] For more details on cults, including definitions and history, see UNODC (2022). Organized Crime in Nigeria: A Threat Assessment. Available at: https://www.unodc.org/conig/uploads/documents/NOCTA_Web_Version_25.09.2023.pdf

[121] Ellis, S. (2016). This Present Darkness: A History of Nigerian Organized Crime. London: Hurst.

[122] UNODC (2022). Organized Crime in Nigeria: A Threat Assessment. Available at: https://www.unodc.org/conig/uploads/documents/NOCTA_Web_Version_25.09.2023.pdf

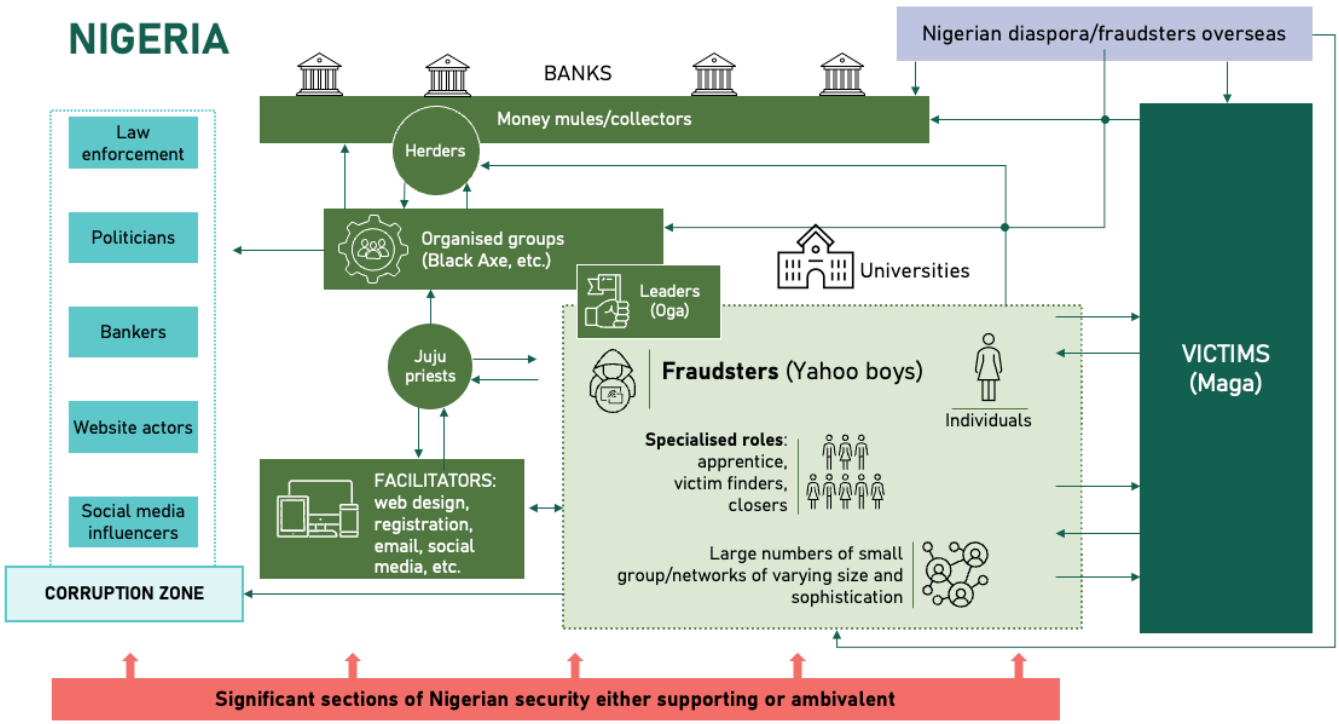
[123] INTERPOL (2023, 8 August). 'Closing ranks on West African organized crime: more than EUR 2 million seized in Operation Jackal'. Available at: https://www.interpol.int/en/News-and-Events/News/2023/Closing-ranks-on-West-African-organized-crime-more-than-EUR-2-million-seized-in-Operation-Jackal

(juju), Lords and Ayes (member operatives – axemen). The involvement of the Black Axe cult provides access to sophisticated mechanisms for laundering money and moving revenue, given the group has also been implicated in human trafficking and drug trafficking.[124] While the Black Axe is the most notorious, the Buccaneers and Supreme Eiye confraternities have also been implicated.

Junior Boboye was described by gardaí as a "high-ranking member of a West African crime group [Black Axe]" when he was jailed in December 2023 for five years for his role in an €800,000 money laundering and fraud operation. In Ireland detectives uncovered more than 1,000 individuals involved in romance and business invoice fraud (most frauds taking place outside Ireland), 838 money mules (recruited and living in Ireland) – although it is believed there could be up to 4000 of these – 63 herders, 50 operational directors and 16 strategists at the top of the network.[125]

Figure 1 shows the organisational structures of fraud networks operating in Nigeria.

Figure 1 Structures of fraud in Nigeria[126]



[124] Crowdstrike (2018). Intelligence Report: CSIR – 18004: Nigerian Confraternities Emerge as Business Email Compromise Threat. Available at: https://www.crowdstrike.com/wp-content/uploads/2020/03/NigerianReport.pdf

[125] Irish Independent (2022). 'Explainer: Who are the Black Axe Gang?' Available at: https://www.youtube.com/watch?v=N7TSP3IE2SQ; Sherry, A. (2023, 14 August). 'Faces of Black Axe international fraud gang members after being busted in Ireland'. Available at: https://www.sundayworld.com/crime/irish-crime/faces-of-black-axe-international-fraud-gang-members-after-being-busted-in-ireland/a357806436.html

[126] Figure developed by Professor Mark Button with Itad design support

4.2. Ghanaian fraud actors

Ghana has similarities to Nigeria in terms of lone actors and loosely organised networks. The key difference is that where fraud is more organised in Ghana, it is usually directed by Nigerian criminal groups that bring in Ghanaian fraudsters.[127]

Younger fraudsters, who are just starting out, tend to work alone, scouring the Internet for resources on how to engage in scams, or seeking information from friends on how to start.[128] Some will continue to work as individuals, in small groups, or for a 'fraud master', who gives them targets.[129] These operations resemble small businesses in which junior fraudsters are 'employed'.[130] There have been several cases of businesslike operations established by Nigerian fraudsters employing Ghanaians; this is discussed in more detail in Section 5.3.[131] Others will form into hierarchical groups, with a division of labour.[132]

Within these hierarchies, there are different roles. 'Browsers' is the most junior role. Their focus is to find victims – scrolling through Facebook, dating sites and other social media to identify suitable targets.[133] When they find targets, these are passed on to others – the 'trust builders'; these are fraudsters that begin conversations and manipulation. The role of the trust builder may be split into two – the 'originator', who tries to get an initial response, and the fraudster, who builds up the relationship.[134] Another fraudster, the 'advanced trust builder', steps in for cases of high value.[135] In addition, there are also 'brokers' – people with wide networks who can connect fraudsters with necessary services and facilitators, including money laundering networks.[136]

The division of labour arises from seniority and experience in conducting fraud, but it is also because some fraudsters are better at certain phases of the scam.[137] However, there is also competition among fraudsters for targets, and fraudsters also try to defraud each other, for example handing over targets that have become suspicious.[138] Although these groups are organised, they are not seen as 'highly organised syndicates', because they are "normal people in the society that lend themselves to this type of crime".[139]

There are more organised groups with a Ghanaian element. These groups will have a larger network to facilitate extortion and tap into the fraudster labour market that exists in Ghana. As one interviewee noted:

> These fraudulent individuals operate in groups to identify potential targets and devise schemes to extort money from them. What sets them apart is their global reach, as they have members located in various countries outside Ghana, predominantly in Europe, Canada, and the USA. This international network allows them to seamlessly

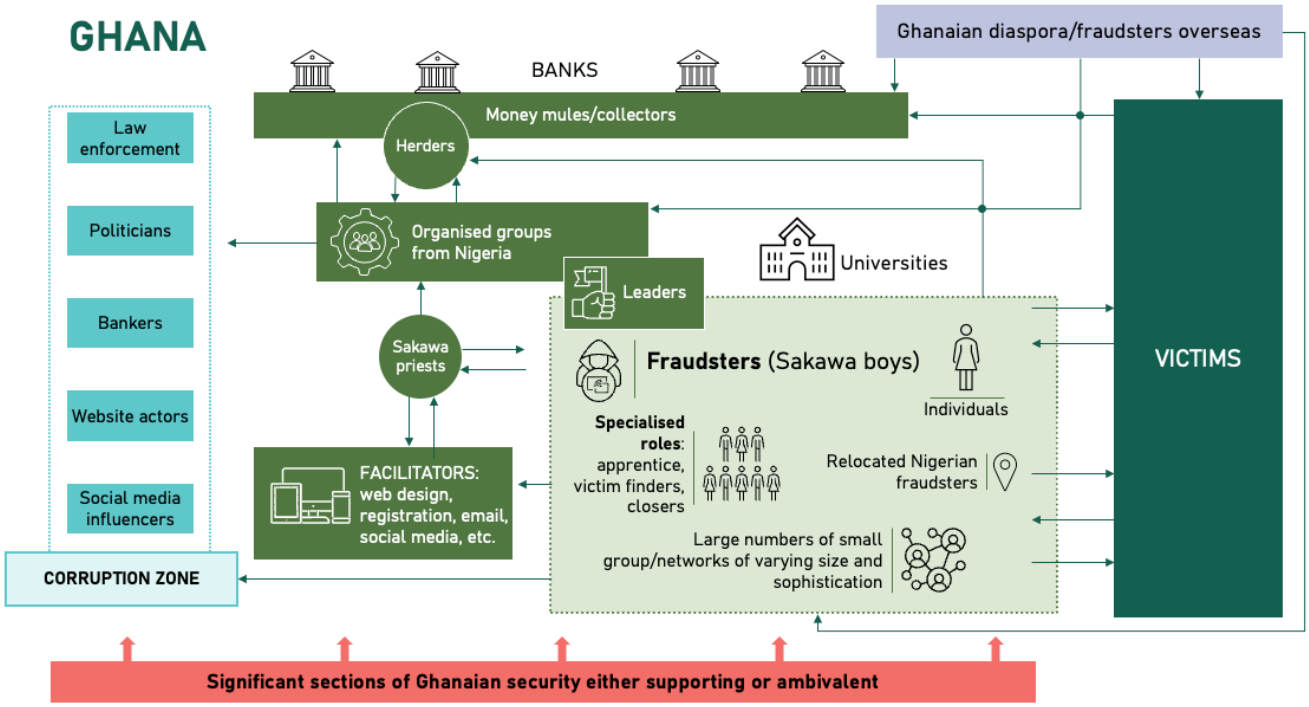
[127] Interview with law enforcement, Ghana.
[128] Interview with an academic, Ghana.
[129] Interview with law enforcement, Ghana.
[130] Interview with law enforcement, Ghana.
[131] Interview with law enforcement, Ghana.
[132] Interview with an academic, Ghana; interview with politician, Ghana; interview with law enforcement, Ghana.
[133] Interview with an academic, Ghana.
[134] Interview with an academic, Ghana.
[135] Interview with an academic, Ghana.
[136] Interview with an academic, Ghana.
[137] Interview with an academic, Ghana.
[138] Interview with an academic, Ghana.
[139] Interview with law enforcement, Ghana.

launder money and engage in other criminal activities to further their fraudulent endeavours. Through this intricate chain, they can pool resources and carry out their illicit activities with greater efficacy.[140]

This enhances the scale and sophistication of fraud schemes. Some argue that "the cafe boys are ready prey for the global syndicates" because they are keen to graduate to more sophisticated crime.[141] This is linked to the perception among Ghanaian law enforcement that organised fraud syndicates originate outside Ghana, using Ghanaian fraudsters as labour, rather than Ghanaian fraudsters having international reach.[142]

Figure 2 shows the organisational structures of fraud networks operating in Ghana.

Figure 2 Structures of fraud in Ghana[143]



4.3. Indian fraud actors

In India, many phone-based scams come from organised call centres, which vary significantly in scale and sophistication. The number of scammers in a centre ranges from a handful to more than 300; set-ups can be small, such as someone's house or a hotel room, or big, such as a purpose-built office space. In the larger centres the organisation is similar to that of a firm, with employees, shifts (including night shifts for international clients), human resources and quality assurance departments, an office for the Chief Executive Officer (CEO), and computers and headsets.[144]

---

[140] Interview with law enforcement, Ghana.

[141] Rubinsztein-Dunlop, S., Robinson, L. and Dredge, S. (2019). 'Meet the scammers: Could this be your online lover?' Available at: https://www.abc.net.au/news/2019-02-11/ghana-meet-the-scammers/10785676

[142] Interview with law enforcement, Ghana.

[143] Figure developed by Professor Mark Button with Itad design support

[144] Interview with cyber expert, India; interview with fraudster, India; Tzani Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R. and Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. *Journal of Forensic and*

Recruitment is facilitated through agencies (see Section 5.3), and employees are given scripts, as well as English and accent training.[145] Often, scammers have performance-based payment incentives, such as taking USD 60 if you manage to make more than USD 1,000 on a call.[146] The incentive structures are often designed in such a way as to make it difficult for people to leave. In one company, employees were paid salaries on the 7th of every month, and commissions were paid 10 days later. If an employee left on the 7th, they would not receive their commission, but if they left 10 days later, they would lose out on 10 days of salary.[147]

The phone scam industry in India is part of a large criminal ecosystem, and individual centres are part of a pan-India network.[148] Similarly to those in Nigeria and Ghana, this decentralised ecosystem has facilitators that offer different services, such as website designers, programmers who develop malware and pop-ups, recruitment agencies, and money mules (money laundering is discussed further in Section 6). There is a black market for SIM cards, phone numbers, victim profiles (with weaknesses highlighted), cultivated fake social media profiles, and even calling scripts. Among call centre workers, you could have 'openers' (those who start the conversation) and 'closers' (those who get the money out of the victim).[149]

This ecosystem is transnational, with reports of support groups operating in the Gulf, China, Hong Kong, Uganda, Canada, the USA and the UK. Accomplices in the target country (including the USA and the UK) act as insiders and are necessary to get personal information on victims, move proceeds, and develop the scams.[150] It is difficult to comment on the level of involvement with OCGs because of the measures used to avoid detection, but one case found links between a call centre and the Lebanon-based Hezbollah militant group.[151] In some cases the managers and financiers of operations in India are based abroad, such as in Dubai or China.[152] One investigation found that the leader of a call centre in India was based in Israel, with managers from Latvia and

---

Investigative Accounting 12(1): 163–78; interview with scamfighter, India; Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231.

[145] Interview with fraudster, India; interview with law enforcement, India; Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0; Tzani Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R. and Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. *Journal of Forensic and Investigative Accounting* 12(1): 163–78; WION (2023, 19 June). 'Delhi Police, FBI bust call centre scam which conned US citizens of $20 million'. Available at: https://www.wionews.com/world/delhi-police-fbi-bust-call-centre-scam-which-conned-us-citizens-of-20-million-605848; Harley, D., Grooten, M., Burn, S. and Johnston, C. (2012). My PC has 32,539 errors: how telephone support scams really work. Virus Bulletin.

[146] Interview with fraudster, India; interview with scamfighter, India; Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231.

[147] Tzani Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R. and Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. *Journal of Forensic and Investigative Accounting* 12(1): 163–78; Liu, X. M. (2021). A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches. *The Coastal Business Journal* 18:1: Article 2.

[148] Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0; Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea; Wen, N. J., Carolyn, M., Ang, J., Jingmin, H. and Shuyan, O. (2021). Uncovering the Workings of Credit-for-Sex Scams. Available at: https://www.mha.gov.sg/docs/hta_libraries/publications/07-crime.pdf

[149] Interview with scamfighter; interview with fraudster, India; interview with cyber expert, India; interview with law enforcement, India; interview with scamfighter, India.

[150] Interview with fraudster, India; interview with journalist, India; interview with law enforcement, India.

[151] Poonam, S. (2018, 2 January). 'The scammers gaming India's overcrowded job market'. Available at: https://www.theguardian.com/news/2018/jan/02/the-scammers-gaming-indias-overcrowded-job-market

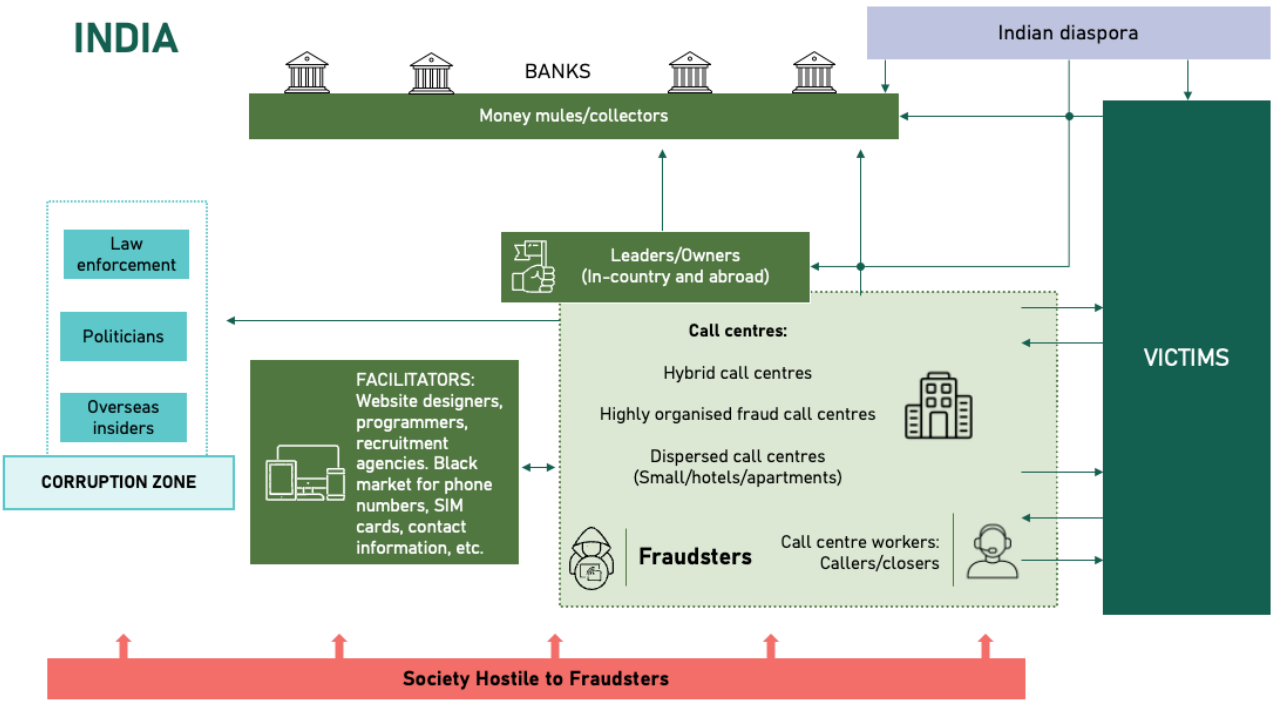
[152] Interview with cyber expert, India; Poonam, S. (2018, 2 January). 'The scammers gaming India's overcrowded job market'. Available at: https://www.theguardian.com/news/2018/jan/02/the-scammers-gaming-indias-overcrowded-job-market

Uzbekistan.[153] There have not been any reports of connections to Nigerian and Ghanaian crime or fraud groups.

In other cases, call centres are set up and managed locally. Case studies show that many owners are ex-employees who worked in bigger fraud centres, or even legal call centres, and who then ventured out and started their own operation because they had developed the right connections, including with lead providers and money launderers.[154] Many centres that started out offering legal business processing outsourcing services entered the scam industry because of its higher returns, and they often conduct fraudulent and legal customer support simultaneously.[155] The barriers to setting up a call centre are not that high, with relatively simple hardware and software requirements. In recent years, call centres have tended to be of smaller scale and more scattered, because of foreign and domestic law enforcement efforts that have disrupted bigger operations (see Section 7).[156] The most extreme example of this is a 'call centre on wheels' in Ahmedabad, Gujarat: scammers were working from moving cars to avoid being tracked and were operating directly from smartphones.[157] The ease of setting up a call centre is also a barrier faced by law enforcement; this issue will be discussed further in Section 7.

Figure 3 shows the organisational structures of fraud networks operating in India.

Figure 3 Structures of fraud in India[158]



[153] WION (2023, 19 June). 'Delhi Police, FBI bust call centre scam which conned US citizens of $20 million'. Available at: https://www.wionews.com/world/delhi-police-fbi-bust-call-centre-scam-which-conned-us-citizens-of-20-million-605848

[154] Wen, N. J., Carolyn, M., Ang, J., Jingmin, H. and Shuyan, O. (2021). Uncovering the Workings of Credit-for-Sex Scams. Available at: https://www.mha.gov.sg/docs/hta_libraries/publications/07-crime.pdf; interview with fraudster, India; Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0

[155] Liu, X. M. (2021). A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches. *The Coastal Business Journal* 18(1): Article 2.

[156] Interview with fraudster, India; interview with scamfighter, India.

[157] Wen, N. J., Carolyn, M., Ang, J., Jingmin, H. and Shuyan, O. (2021). Uncovering the Workings of Credit-for-Sex Scams. Available at: https://www.mha.gov.sg/docs/hta_libraries/publications/07-crime.pdf

[158] Figure developed by Professor Mark Button with Itad design support

5. Fraudsters

In all three countries, fraudsters tend to be young and educated, most are male, and they choose to engage in fraud for economic reasons. This section explores the demographic details of fraudsters that emerged from the research, as well as their motivations and how they are recruited.

5.1. Demographics of fraudsters

In Nigeria, the majority of fraudsters are based in the south of the country – usually in urban areas.[159] One interviewee quantified the north-south divide – out of 100 convictions, at least 90 are from the south.[160] This is linked to how fraud is perceived in different parts of the country, as well as to access to technology.

Although the dominant group is males aged 19–35, new fraudsters are as young as 13, with evidence of 10–12-year-olds being trained.[166] Many fraudsters are university students or graduates, particularly those involved in more sophisticated scams, such as BEC, that target businesses and organisations and leverage the intelligence and strategic reasoning gained at university.[167]

The role of women

Although the majority of fraudsters are male, the number of women involved is increasing.[161] A study that interviewed 17 female undergraduate students in Nigeria found found that those who participated in online fraud had been initiated and supervised by male relatives, boyfriends, mentors or associates.[162] Female fraudsters are particularly involved in targeting male victims in romance schemes, providing a face and a voice to entice victims, with male fraudsters often taking over once the victim has been baited.[163] The drivers for women's involvement are the same as those for men – financial gain and peer pressure – but gender norms apply both online and offline, which influences the extent to which women engage in cybercrime.[164] However, in Ghana the digital landscape of fraud is allowing women to evade the societal and legal repercussions of their involvement in criminal activity, and they are becoming more entrepreneurial.[165]

---

[159] Interview with EFCC, Nigeria; interview with EFCC, Nigeria; interview with fraudster, Nigeria; interview with EFCC, Nigeria; interview with NGO, Nigeria; interview with EFCC, Nigeria.

[160] Interview with EFCC, Nigeria.

[161] Interview with NGO, Nigeria.

[162] Ogunleye, Y. O., Ojedokun, U. A. and Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology* 13(2): 309–25; interview with ex-fraudster, Nigeria.

[163] Interview with fraudster, Nigeria; interview with ex-fraudster, Nigeria.

[164] Ogunleye, Y. O., Ojedokun, U. A. and Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology* 13(2): 309–25.

[165] Abubakari, Y. (2023). The Espouse of Women in the Online Romance Fraud World: Role of Sociocultural Experiences and Digital Technologies. *Deviant Behavior* 45(5): 708–35. DOI: 10.1080/01639625.2023.2263137.

[166] Interview with EFCC, Nigeria; interview with NGO, Nigeria.

[167] Interview with EFCC, Nigeria.

An interview with law enforcement stated that 80% of male university students are involved in cybercrime.[168] Students involved in fraud tend to be enrolled in engineering or computer science programmes.[169]

The demographics of those involved in fraud are diversifying. For example, university lecturers have been arrested, as have 'corpers' (those engaged in military service) and bankers.[170] In some cases, these individuals started as fraudsters while they were students and have carried on engaging in fraud alongside their legitimate activities.[171]

Younger fraudsters tend to be enrolled in school, although many stop going to classes, instead spending their time engaged in fraud. Some of these younger scammers have educated themselves on how to scam online, as they are very 'tech-savvy'.[172]

The demographics of fraudsters in Ghana have some similarities to those of Nigeria. Universities are also hotspots for young people involved in fraud, particularly the University of Ghana and Kwame Nkrumah University of Science and Technology, because of their focus on engineering and technology programmes.[173] However, there is more diversity among fraudsters in Ghana. "They range from educated individuals to those without much formal education, and they can be both employed or unemployed".[174] Some even maintain legitimate businesses to disguise their fraudulent activities.[175]

Primarily fraudsters are from urban areas, with Accra a major centre for fraud.[176] Other hotspots include Tamale, Kumasi, Takoradi, Cape Coast, Kasoa, Winneba, Tema, Sunyani, Sogakope, Assin-Manso, Assenua, Mankessim, Akosombo, Wenchi and Jirapa.[177] There is also increasing activity in the northern region and the Volta region, because security agencies do not have the technical capability to tackle cyber fraud in these regions.[178]

In Indian call centres, the standard profile of people working as scammers is young (between the ages of 18–30, with one report of a fraudster as young as 16) and tech-savvy, with a high level of education (usually college-level) and with English-speaking skills.[179] In some cases it has been observed that fraudsters start out on a part-time basis but eventually make it their main career, and can even drop out of college to dedicate more time to fraud.[180] The demographic is a majority of males, especially for call centres that run in the evenings and nights to target international victims, because of norms around women's safety in India. Nonetheless, in many

---

[168] Interview with EFCC, Nigeria.

[169] Interview with EFCC, Nigeria.

[170] Interview with EFCC, Nigeria.

[171] Interview with EFCC, Nigeria.

[172] Interview with NGO, Nigeria.

[173] Interview with law enforcement, Ghana; interview with law enforcement, Ghana.

[174] Interview with law enforcement, Ghana.

[175] Interview with law enforcement, Ghana.

[176] Key areas cited include Teshie, Osu, Amasaman, Pantang, Amarhia, Sunyani, Airport, Spintex, La Paz, Adenta and Madina areas.

[177] Interview with law enforcement, Ghana; interview with law enforcement, Ghana.

[178] Interview with law enforcement, Ghana.

[179] Interview with cyber expert, India; interview with journalist, India; Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0; Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea; interview with fraudster, India; interview with fraudster, India; interview with law enforcement, India.

[180] Interview with fraudster, India; interview with law enforcement, India; Economic Times (2021, 4 June). 'How scammers are targeting vulnerable and desperate during India's COVID crisis'. Available at: https://economictimes.indiatimes.com/news/india/how-scammers-are-targeting-the-vulnerable-and-the-desperate-during-indias-covid-crisis/history-of-scams/slideshow/83228982.cms

centres there is a sizeable female workforce, ranging from 5% to 40% of the staff.[181] Of particular note is the preference for women from the north-east of India, who have better English-speaking skills.[182] There have been reports of fraud centres in all major cities of India, including Delhi, Kolkata, Mumbai, Pune, Chandigarh, Hyderabad, Bangalore and Ahmedabad, and the workforce can include both rural migrants and the urban lower and middle classes.[183] There are also some scam hubs emerging in rural areas which employ the local village population. [184]

5.2. Motivations

In all three countries, economic drivers are the core motivation to become involved in fraud, given the high rates of youth unemployment in Nigeria, Ghana and India. However, in all three countries aspiration also plays a role, perhaps linked to the educational background of the fraudsters. There is also social value that arises from being a fraudster and being able to displace wealth, particularly in Nigeria and Ghana.

Poverty is frequently cited as a driver for young people to become involved in fraud in Nigeria. However, as discussed above, aspiring fraudsters still need to have access to technology to become involved. Adogame (2009) argues that "electronic mail technology as new public spaces is still a luxury afforded to the upwardly mobile youth, the educated elites and students".[185] As many fraudsters are attending university, poverty cannot be the main driver.[186] Accordingly, the driver is unmet aspirations, which has parallels with other forms of organised crime in Nigeria.[187] A study by Akinyetun (2021) finds that "unguided Nigerian youth are compelled to resort to crime as a means of bridging the gap between their current reality and the Nigeria of their aspirations".[188] One interviewee noted that many are "probably motivated by what they see on social media, and they want to join the bandwagon".[189] There are also indications that Nigerians in tertiary education experience parental pressure to succeed, and there is evidence of parents pushing their children to become involved in fraud (see Section 8.2).[190]

Those involved in fraud cite the difficulties of being a young, unemployed graduate in Nigeria as a key driver.[191] The share of youth aged 15–29 not in education, employment or training (NEET)

---

[181] Interview with journalist, India; interview with law enforcement, India; interview with law enforcement, India; Tzani Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R. and Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. *Journal of Forensic and Investigative Accounting* 12(1): 163–78; Wen, N. J., Carolyn, M., Ang, J., Jingmin, H. and Shuyan, O. (2021). Uncovering the Workings of Credit-for-Sex Scams. Available at: https://www.mha.gov.sg/docs/hta_libraries/publications/07-crime.pdf

[182] Interview with cyber expert, India; interview with law enforcement, India.

[183] Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0; Liu, J., Pun, P., Vadrevu, P. and Perdisci, R. (2023). Understanding, Measuring, and Detecting Modern Technical Support Scams. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*: 18–38; Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea; Vaidyanathan, R. (2020, 8 March). 'Confessions of a call-centre scammer'. Available at: https://www.bbc.com/news/stories-51753362

[184] Interview with cyber expert, India.

[185] Adogame, A. (2009). The 419 Code as Business Unusual: Youth and the Unfolding of the Advance Fee Fraud Online Discourse. *Asian Journal of Social Science* 37(4): 551–73.

[186] Interview with EFCC, Nigeria.

[187] This is discussed in relation to human trafficking in Jesperson, S. et al. (2019). Human Trafficking: An Organised Crime? London: Hurst.

[188] Akinyetun, T. (2021). Poverty, Cybercrime and National Security in Nigeria. *Journal of Contemporary Sociological Issues* 1(2): 86–109.

[189] Interview with EFCC, Nigeria.

[190] Akeusola, B. N. (2023). Parental Pressure and Cybercrime Engagement among Youth in Nigerian Tertiary Institutions. *KIU Journal of Social Sciences* 9(3): 117–25.

[191] Interview with EFCC, Nigeria.

was 26.2% in 2019.[192] For example, "maybe someone went to school or university and you finish school or university, you work hard, walk the streets looking for a job, and at the end of the day, no work, no job, nothing, nothing, so what do you expect?"[193] For many individuals, cybercrime becomes a means of survival in the face of economic hardships and lack of employment opportunities.[194] Similarly, an NGO working on cybercrime stated that:

> [In] many of the places where we are working, we've found that because of the situation of the economy, people are looking for a way to survive, and then the breakdown of family ties and parental care, a lot of young people have delved into these things to survive, to fend for themselves.[195]

In West Africa, a major driver is showing off a lavish, materialistic lifestyle. Underpinning this is a desire to 'get rich quick', with money the main motivation.[196] As one interviewee stated, "everyone wants to have money, everyone wants to drive a car, everyone wants to have a house".[197] Seeing friends making money easily entices those doing the right thing:

> The upcoming generation what they see is what they replicate. When they see their older ones, you know, living the fancy life, living a life that the source of wealth cannot be ascertained, they see it as a way of life.[198]

There tends to be a difference in motivation between students and graduates involved in fraud – for students the driver is largely materialistic, whereas for graduates the motive is primarily to get by.

For those experiencing guilt, it is easier to disassociate from cross-border fraud, because the victim is far away and there is a low chance of getting caught and arrested (see Section 7). Many believe that the victim already has a lot of money and can afford to part with some of it.[199] In fact, some fraudsters claimed to stop the call if they felt the customer couldn't afford it.[200] This is also perhaps why some (though not all) claim to avoid targeting people of Indian origin abroad.[201] Nonetheless, as described in Section 3, the choice of victim and the types of fraud are diverse, and in many cases frauds are targeted specifically at the diaspora.

---

[192] International Labour Organization (2023). ILO Youth Country Briefs: Nigeria. Available at: https://webapps.ilo.org/wcmsp5/groups/public/---ed_emp/documents/publication/wcms_886409.pdf

[193] Interview with ex-fraudster, Nigeria.

[194] Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian Social Science* 13(4): 19–29.

[195] Interview with NGO, Nigeria.

[196] Interview with EFCC, Nigeria; interview with EFCC, Nigeria; interview with NGO, Nigeria; interview with NGO, Nigeria; interview with EFCC, Nigeria; Peace, F. W., Egharevba, M. E. and George, T. O. (2022). Sociological Investigation of Factors Driving Cybercrime Among Undergraduates with Severe Implication in the Educational System in Nigeria. *Proceedings of SOCIOINT 2022 – 9th International Conference on Education & Education of Social Sciences*; Egole, A. and Okamgba, J. (2023, 5 December). 'Worsening youth unemployment triggers fresh cybercrime, voodoo wave'. Available at: https://punchng.com/worsening-youth-unemployment-triggers-fresh-cybercrime-voodoo-wave/

[197] Interview with fraudster, Nigeria.

[198] Interview with EFCC, Nigeria.

[199] Interview with fraudster, India; interview with fraudster, India; Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0; Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea; interview with scamfighter, India.

[200] Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0; Microsoft (2021). Global Tech Support Scam Research. Available at: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2021/07/MSFT-2021-Global-Tech-Support-Scam-Research-Report.pdf

[201] Interview with fraudster, India.

Economics as a primary driver for engaging in fraud is also the case in Ghana.[202] The NEET rate for 15–29-year-olds in Ghana was 22.3% in 2017 – almost 8% higher than the 2013 figure (14.5%).[203] Fraud is hence viewed as an avenue for income.[204] This exists on a spectrum. Given there is evidence of less educated individuals engaging in fraud, poverty is more of a factor than in Nigeria, with some fraudsters dwelling in Accra slums.[205] However, others are seeking wealth, and they see fraud as a strategy to earn money and live a "higher lifestyle than what they have" quickly and easily.[206] This is less prevalent than the 'get rich quick' attitude of Nigeria; although there are examples of fraudsters driving flashy cars, there is more association with using the proceeds of fraud to take care of their families, including buying food, paying for siblings' education, and maintaining shelter.[207]

Some fraudsters in Nigeria and Ghana justify their involvement in fraud on the basis of payback for colonialism "defrauding victims from the West of what belongs to their forefathers".[208] However, one interview argued that although this is expressed as a motivation, the real driver is money.[209] Other strategies to justify involvement are discussed in Section 8.3. At a lesser scale, some fraudsters claim to be motivated by revenge or payback against organisations or individuals they believe have wronged them.[210] Some have even been defrauded themselves.[211] Other motivations include "financial gain, desperation, lack of moral or ethical principles, and sometimes a misguided sense of entitlement".[212]

The majority of young people in India who join scam call centres initially think they are legitimate and legal (see Section 5.3). Scammers may not initially know that they are being hired to an illegal call centre, but they find out very quickly, usually during training. At this point some leave, with one report showing that the average retention rate for a centre was just two months.[213] This may be due to poor working conditions, but many ex-fraudsters have admitted to feeling guilt and shame.[214] However, most reports show that the high incentives and salaries (especially in a country with chronic youth unemployment and low job prospects for educated youth) induce people to stay, even if they did not realise it was fraud when they joined.[215] In India the youth unemployment rate has been rising over several decades, and unemployment among

---

[202] Interview with an academic, Ghana; interview with law enforcement, Ghana; interview with law enforcement, Ghana; interview with law enforcement, Ghana; interview with law enforcement, Ghana; interview with government, Ghana; Adebayo, B. (2023, 15 August). 'Sakawa Boys: Meet Ghana's online romance scammers'. Available at: https://www.context.news/digital-rights/sakawa-boys-meet-ghanas-online-romance-scammers

[203] International Labour Organization (2023). ILO Youth Country Briefs: Ghana. Available at: https://webapps.ilo.org/wcmsp5/groups/public/---ed_emp/documents/publication/wcms_886402.pdf

[204] Interview with law enforcement, Ghana.

[205] Interview with an academic, Ghana; interview with law enforcement, Ghana; interview with law enforcement, Ghana.

[206] Interview with law enforcement, Ghana; interview with law enforcement, Ghana.

[207] Interview with law enforcement, Ghana.

[208] Interview with law enforcement, Ghana; interview with law enforcement, Ghana; interview with law enforcement, Ghana.

[209] Interview with law enforcement, Ghana.

[210] Interview with law enforcement, Ghana.

[211] Interview with fraudster, Ghana.

[212] Interview with law enforcement, Ghana.

[213] Economic Times (2021, 4 June). 'How scammers are targeting vulnerable and desperate during India's COVID crisis'. Available at: https://economictimes.indiatimes.com/news/india/how-scammers-are-targeting-the-vulnerable-and-the-desperate-during-indias-covid-crisis/history-of-scams/slideshow/83228982.cms; Van Nguyen, T. (2022). The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. *Trends in Organized Crime* 25(2): 226–47.

[214] Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0; Microsoft (2021). Global Tech Support Scam Research. Available at: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2021/07/MSFT-2021-Global-Tech-Support-Scam-Research-Report.pdf; interview with scamfighter, India.

[215] Interview with fraudster, India; interview with fraudster, India; interview with fraudster, India; interview with law enforcement, India; interview with scamfighter, India.

educated youth is particularly high (28.7% in 2022).[216] In a testimony, one fraudster said, "Sometimes I feel it's wrong and I want to quit, but the money is too good […] I can't think of another way to make this kind of money".[217] In some cases, fraudsters have switched jobs once they made enough money.[218]

Despite the fact that, for many, scamming is a choice made out of necessity, there are those who enjoy scamming and do not feel guilt or remorse. They may even have aspirations to open their own centres and expand the business.[219] As seen in Section 4, many fraud centres are formed by employees of another centre. An interview with a fraudster revealed that they enjoy working for many centres as a contractor and are constantly shifting bases.[220] Although scammers may experience guilt initially, the earning potential and normalisation of fraud among many peer groups can keep them within the industry. Indian youth are aspirational and spend their earnings on lifestyle goods, especially because of the growing influence of social media, including displays of wealth on Instagram. The money and the job, which requires English and technology skills and allows a certain degree of freedom, provides social signalling power. They are able to achieve this lifestyle with relatively little effort.[221]

5.3. Recruitment

There are varying levels of willingness to engage in fraud. As discussed above, most recruits in India are not initially aware that they are being employed by a scam call centre. This is less common in Nigeria and Ghana, where young people may seek out existing fraudsters to mentor them, although there is some evidence of forced recruitment in Ghana, including of Nigerians.

In Nigeria, most prospective fraudsters choose to become involved; there is less active recruitment.[222] Young people will call friends they know are involved in fraud and get into it that way.[223] Others approach people known to be fraudsters, seeking a mentor to guide them.[224] Where there is active recruitment, this is also done through peer groups, and universities are central to the recruitment of fraudsters.[225] There is an element of peer pressure: "they are being lured by friends or a group of friends to join a particular act as they have seen it as the only source that can give them what we call quick money".[226] Wider research has highlighted the significant importance of regular encounters between yahoo boys and young individuals in introducing the latter to cybercrime.[227]

---

[216] International Labour Organization (2024). India Employment Report 2024: Youth employment, education and skills. Available at: https://webapps.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---sro-new_delhi/documents/publication/wcms_921154.pdf

[217] Interview with fraudster, India.

[218] Interview with fraudster, India; Liu, X. M. (2021). A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches. *The Coastal Business Journal* 18(1): Article 2.

[219] Interview with scamfighter, India; Van Nguyen, T. (2022). The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. *Trends in Organized Crime* 25(2): 226–47.

[220] Interview with fraudster, India.

[221] Interview with cyber expert, India; interview with journalist, India; interview with fraudster, India; interview with law enforcement, India; interview with law enforcement, India.

[222] Adejoh, S. O., Alabi, T. A., Adisa, W. B. and Emezie, N. M. (2019). "Yahoo Boys" Phenomenon in Lagos Metropolis: A Qualitative Investigation. *International Journal of Cyber Criminology* 13(1): 1–20.

[223] Interview with EFCC, Nigeria.

[224] Interview with EFCC, Nigeria.

[225] Interview with EFCC, Nigeria.

[226] Interview with EFCC, Nigeria.

[227] Adejoh, S. O., Alabi, T. A., Adisa, W. B. and Emezie, N. M. (2019). "Yahoo Boys" Phenomenon in Lagos Metropolis: A Qualitative Investigation. *International Journal of Cyber Criminology* 13(1): 1–20.

In Ghana, existing fraudsters recruit through their networks and social circles, leveraging trust and social connections to persuade others to get involved without understanding the consequences or risks.[228] As in Nigeria, many networks are hierarchical, with new recruits paying a percentage of their revenue upwards, which means that recruiting additional fraudsters increases income. Social media is also a tool for grooming new fraudsters,[229] and text message blasts have offered guidance in becoming a fraudster.[230] Aspiring fraudsters learn the trade through training and mentorship from existing fraudsters.[231] They can also learn by studying online resources, tutorials and guides that provide information on fraudulent techniques, tactics and tools; and they can participate in online forums, chat rooms and communities dedicated to cybercrime.[232]

There are also cases of Nigerian fraudsters setting up in Ghana, recruiting Ghanaians.[233] In one case, a Nigerian fraudster rented an apartment and hired young Ghanaians, paying them a fixed monthly salary, and their 'job' was to defraud people.[234] Other nationalities are also brought to Ghana to engage in fraud, because the criminal justice system is seen to be unable to manage, fraudsters can disguise their activities, and even if they are arrested, they will be released in 48 hours.[235] One interviewee recounted helping a German, who presented himself as a victim of fraud but was actually a fraudster himself who lived in Ghana.[236]

In contrast to Nigeria, there is some evidence of forced recruitment into fraud in Ghana, although this is not at the same scale as the evidence in Southeast Asia.[237] Some are looking for work and are recruited by fraudsters, and they need to earn their freedom by engaging in fraud.[238] There are also cases of Nigerians being duped into travelling to Ghana expecting to find well-paid corporate jobs but instead being forced to meet daily targets through cyber fraud.[239] In July 2023, Ghana's Anti-Trafficking Unit rescued 31 Nigerian men who had been deceived in this way; they had their identity documents and personal belongings seized and were locked in a warehouse alongside others.[240] In some cases, however, narratives of forced recruitment are used as a justification for engagement in fraud.

In contrast to Nigeria and Ghana, in India many call centres follow a formal recruitment process, which is done by in-house or contracted recruitment agencies, who earn a commission on placing jobseekers. This network of recruiters is vast and growing and has become part of the fraud ecosystem (see Section 4.3).[241] These agencies have CVs and biodata of potential

---

[228] Interview with law enforcement, Ghana.

[229] Interview with law enforcement, Ghana.

[230] Text message blasts are a marketing strategy whereby a message is sent to a large batch of phone numbers; interview with politician, Ghana.

[231] Interview with law enforcement, Ghana.

[232] Interview with law enforcement, Ghana.

[233] Interview with law enforcement, Ghana; interview with government, Ghana; interview with law enforcement, Ghana.

[234] Interview with law enforcement, Ghana.

[235] Interview with law enforcement, Ghana.

[236] Interview with an academic, Ghana.

[237] Interview with law enforcement, Ghana; interview with politician, Ghana; interview with law enforcement, Ghana.

[238] Interview with politician, Ghana.

[239] ActionAid (2023, 27 July). 'Nigerians trafficked to Ghana and forced to work as cyber-criminals for ruthless gangs'. Available at: https://actionaid.org/stories/2023/nigerians-trafficked-ghana-and-forced-work-cyber-criminals-ruthless-gangs

[240] Ibid.

[241] Van Nguyen, T. (2022). The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. Trends Organ Crim 25, 226–247; Economic Times (2021, 4 June). 'How scammers are targeting vulnerable and desperate during India's COVID crisis'. Available at: https://economictimes.indiatimes.com/news/india/how-scammers-are-targeting-the-vulnerable-and-the-desperate-during-indias-covid-crisis/history-of-scams/slideshow/83228982.cms

candidates, which they find online or receive from jobseekers themselves.[242] Call centres can advertise themselves using newspaper ads, posters, adverts, social media, cross-referrals and even (in one case) a formal campus job placement interview.[243] It is important to note here that overwhelmingly, the evidence shows that candidates are not aware that they are being recruited to conduct fraud. The agencies and call centres advertise themselves as legitimate, and do not use the words 'scam' or 'victims', instead using terms such as 'Amazon processing' and 'customers'. Often they do not mention the name of the company, and they communicate via text messages,[244] attracting candidates with the offers of high salaries and incentives.[245]

In some cases fraudsters are recruited through word of mouth, in which case they are more likely to know the true nature of the work. If one person gets drawn in, so do their peers, and there is not much formal training.[246] The high earning potential attracts others, especially in rural areas. Some parts of the country have become major scam hubs, with the entire village or block involved and participating.[247]

Although the evidence reviewed shows no indication of forced labour or slavery, there are some reports of extremely poor working environments. Sources have reported on centres that put pressure on employees to meet targets through threats of firing, physical violence, not allowing employees to go home or use the toilet, or forcing them to come back after quitting if they do not complete their one-year contract. Staff are unable to report this abuse because the centre is illegal, indicating that such crimes go underreported.[248]

The potential income from fraud provides a draw in all three countries which is difficult to deter. Fraud also provides a form of skilled employment, which is rare for young people in Nigeria, Ghana and India.

---

[242] Interview with fraudster, India; interview with fraudster, India.

[243] Interview with scamfighter, India; Liu, J., Pun, P., Vadrevu, P. and Perdisci, R. (2023). Understanding, Measuring, and Detecting Modern Technical Support Scams. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*: 18-38; Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231; Van Nguyen, T. (2022). The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. *Trends in Organized Crime* 25(2): 226–47; Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea

[244] Economic Times (2021, 4 June). 'How scammers are targeting vulnerable and desperate during India's COVID crisis'. Available at: https://economictimes.indiatimes.com/news/india/how-scammers-are-targeting-the-vulnerable-and-the-desperate-during-indias-covid-crisis/history-of-scams/slideshow/83228982.cms

[245] Interview with fraudster, India; interview with fraudster, India; interview with scamfighter, India.

[246] Interview with cyber expert, India; interview with journalist, India; interview with law enforcement, India; interview with law enforcement, India.

[247] Interview with cyber expert, India.

[248] Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231; Van Nguyen, T. (2022). The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. *Trends in Organized Crime* 25(2): 226–47; Liu, X. M. (2021). A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches. *The Coastal Business Journal* 18(1): Article 2.

6. Proceeds of fraud

Various tactics are used to disguise the proceeds of fraud and transfer it to fraudsters in the country from where the fraud originated. The research identified some strategies, but more research is needed in this area.

6.1. Nigeria

In Nigeria, the revenue from fraud used to be transferred through Western Union and MoneyGram, but this has become too difficult, because receiving funds requires a unique bank verification number or national identification number.[249] As a result, organised groups are playing a role in laundering fraud revenue using a variety of methods including money mules with often diverse networks, through to trade-based money laundering. One tactic, particularly for money leaving USA accounts, is for funds to be transferred to China, where it is used to purchase goods, which are sent to Nigeria and other countries to be sold.[250] However, Nigeria's Economic and Financial Crime Commission (EFCC) has recently established contact with the Chinese embassy to investigate these cases. There are also cases of successful fraudsters establishing legitimate business to cover up their illicit revenues.[251]

Cryptocurrencies are being used to move the proceeds of fraud to Nigeria. When cryptocurrency is transferred into fiat currencies (currencies issued by governments), the exchanger is aware of the illegality of funds and buys at a lower rate.[252] Politicians have also been identified as a conduit for laundering the proceeds of fraud.[253]

Although the majority of fraudsters originate from the southern regions of Nigeria, there is evidence of interface with northerners when it comes to proceeds of fraud. Unofficial bureaux de change have been offering black market rates for currency exchange in Lagos and Abuja.[254] However, attempts to improve Nigerian monetary policy are making currency trading less profitable.[255]

6.2. Ghana

The hierarchical structures of fraud have established systems for the divisions of income. In Ghana, the person who starts the conversation with the victim or client receives 40% of any returns received, and the remainder is shared among other fraudsters involved and those higher up in the hierarchy.[256] Previously, smaller transactions had not drawn much attention.[257] The introduction of the Ghana Card has made this more challenging. From July 2022, the Ghana Card has been the only identification card that can be used to undertake transactions at all Bank of Ghana licensed and regulated financial institutions, including banks, specialised deposit-taking

---

[249] Interview with EFCC, Nigeria.

[250] Interview with EFCC, Nigeria.

[251] Interview with EFCC, Nigeria.

[252] Interview with EFCC, Nigeria.

[253] Interview with EFCC, Nigeria.

[254] Ajala, E. B. (2007). Cybercafes, Cybercrime Detection and Prevention. *Library Hi Tech News* 24(7): 26–29.

[255] Monye, E. (2024, 18 January). 'Why Nigeria's Controversial Naira Redesign Policy Hasn't Met Its Objectives'. Available at: https://carnegieendowment.org/2024/01/18/why-nigeria-s-controversial-naira-redesign-policy-hasn-t-met-its-objectives-pub-91405; Ohuocha, C. (2024, 26 February). 'Nigeria outlaws street-trading by FX bureaus in new rules to stem naira slide'. Available at: https://www.cnbcafrica.com/2024/nigeria-outlaws-street-trading-by-fx-bureaus-in-new-rules-to-stem-naira-slide/

[256] Interview with an academic, Ghana.

[257] Interview with law enforcement, Ghana.

institutions, non-deposit-taking financial institutions, payment service providers and dedicated electronic money issuers, forex bureaus and credit reference bureaus.[258] As a result, other strategies are being employed to transfer revenue back into Ghana.

One interview noted that fraudsters have international networks that facilitate the movement of money – referred to as 'pick up':

> Sometimes victims are sceptical about sending money across, for instance, to Ghana. So what they do is that they […] contact their network […] in the UK or the US. So the victim will send the money to them […] and usually this international network will share accounts, they create accounts with schooling identities and stuff like that, and they use that to take the money and send part of it to their networks in Ghana.[259]

In one case, six ringleaders of a Ghana-based criminal enterprise were arrested on charges of laundering more than USD 50 million through scams targeting the elderly, BECs and fraudulent relief loans, with four of them controlling more than 45 bank accounts where the majority of the funds were deposited between 2013 and 2020.[260]

There are also instances of victims being told to send money to a second victim, who does not realise they are also a victim, effectively becoming a money mule.[261] The purchase of vehicles in Ghana is also an effective method, because no one is surprised by cash purchases, and car dealerships rarely have security mechanisms in place to check identities or the source of funds.[262] Hawala, a method of moving money without physical money moving, is also playing a bigger role in Ghana, often through the United Arab Emirates and China.[263] In these cases, hawala brokers receive payment and contact another hawala broker in the destination country, asking them to pay the intended recipient. The transfers are anonymous and work on a system of balancing the books of hawala brokers without moving money directly.

6.3. India

In India, the profits earned from fraud are distributed among all the players in the ecosystem, but with a heavy skew towards the 'top brass'. Profits from international scams can be big, because of the cheap labour costs in India; management rarely get caught during raids and investigations, but they pocket most of the proceeds.[264] Workers can get between 5% and 10% of what they steal, but this may be as high as 30%–40%, with the share rising in line with the amount stolen, as an incentive.[265] The remaining profit goes to the top. The inequality can be stark, with one case finding a scammer who made one rupee for every dollar he stole, while a scam boss

---

[258] Interview with politician, Ghana.

[259] Interview with an academic, Ghana.

[260] Citi Newsroom (2021, February 18). 'US busts '$50 million Ghana-based cyber fraud scam". Available at: https://citinewsroom.com/2021/02/us-busts-50m-ghana-based-cyber-fraud-scam/

[261] Interview with an academic, Ghana.

[262] Interview with government, Ghana.

[263] Interview with law enforcement, Ghana.

[264] Interview with fraudster, India; interview with fraudster, India; interview with journalist, India.

[265] Interview with scamfighter, India; Wen, N. J., Carolyn, M., Ang, J., Jingmin, H. and Shuyan, O. (2021). Uncovering the Workings of Credit-for-Sex Scams. Available at: https://www.mha.gov.sg/docs/hta_libraries/publications/07-crime.pdf; Economic Times (2021, 4 June). 'How scammers are targeting vulnerable and desperate during India's COVID crisis'. Available at: https://economictimes.indiatimes.com/news/india/how-scammers-are-targeting-the-vulnerable-and-the-desperate-during-indias-covid-crisis/history-of-scams/slideshow/83228982.cms

could make around 240,000 GBP a month.[266] Nonetheless, due to high unemployment, especially among educated youth, this salary is attractive to most fraudsters. An analysis of tech support fraud in India found that the median revenue of a successful call is 200 GBP, which implies that the target success rate for a centre to be profitable is 15%, which is quite high. Research shows that the success rate is around 1%–2%, implying that further investigation is needed into the proceeds and financials of fraud centres in India.[267]

Methods used to move revenue include setting up multiple bogus accounts to bounce money around, so that the trail goes cold and difficult to track.[268] For example, an investigation of a transnational fraud group with actors in India found 48 bank accounts of shell companies holding around 584 crore rupees (55.8 million GBP). People were paid around 1600 GBP to open an account for a shell company with their personal information.[269] Gift cards are overwhelmingly the dominant mode to move money without being traced (because they do not require identification verification and they are easily available), but other methods include iTunes, cryptocurrency, and prepaid debit cards.[270] If the scammer is in another country, they could use mules to spend the card and later pay the money to scammers, or scammers can use the card directly themselves.[271] Personal identifying information stolen from the web or through scams is also used to conduct wire transfers using fake names.[272] It is important to note that colleagues in the victim country are essential for money laundering across borders, and reports have found co-conspirators in the USA and the UK liquidating and laundering funds.[273] Moreover, evidence shows that money can get routed through countries such as China, Hong Kong and Pakistan.[274] There are groups in the ecosystem that specialise in laundering through gift cards, credit cards, online financial services, wire transfers, and even mail services such as FedEx and UPS.[275]

Although different methods are used to move the proceeds of fraud back to the country conducting the fraud, most require the involvement of an international network. Pursuing nodes in the money laundering network has been a key strategy in the USA, where fraudsters have been prosecuted using anti-money laundering legislation. However, the international networks of fraudsters are not well understood.

---

[266] Microsoft (2021). Global Tech Support Scam Research. Available at: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2021/07/MSFT-2021-Global-Tech-Support-Scam-Research-Report.pdf; Liu, X. M. (2021). A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches. *The Coastal Business Journal* 18(1): Article 2.

[267] Liu, J., Pun, P., Vadrevu, P. and Perdisci, R. (2023). Understanding, Measuring, and Detecting Modern Technical Support Scams. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*: 18-38.

[268] Vaidyanathan, R. (2020, 8 March). 'Confessions of a call-centre scammer'. Available at: https://www.bbc.com/news/stories-51753362

[269] Poonam, S. (2018, 2 January). 'The scammers gaming India's overcrowded job market'. Available at: https://www.theguardian.com/news/2018/jan/02/the-scammers-gaming-indias-overcrowded-job-market

[270] Interview with journalist, India; interview with law enforcement, India.

[271] Chaganti, R., Bhushan, B., Nayyar, A. and Mourade, A. (2021). Recent Trends in Social Engineering Scams and Case Study of Gift Card Scam. arXiv preprint. arXiv:2110.06487.

[272] Johnson, B. M. (2022, 10 April). 'Rise of the scam baiter – fall of the scammers'. Available at: https://www.linkedin.com/pulse/rise-scam-baiter-fall-scammers-bronwyn-may-johnson-mba-/

[273] Interview with fraudster, India; Johnson, B. M. (2022, 10 April). 'Rise of the scam baiter – fall of the scammers'. Available at: https://www.linkedin.com/pulse/rise-scam-baiter-fall-scammers-bronwyn-may-johnson-mba-/; interview with scamfighter, India.

[274] Interview with law enforcement, India; interview with fraudster, India.

[275] Liu, J., Pun, P., Vadrevu, P. and Perdisci, R. (2023). Understanding, Measuring, and Detecting Modern Technical Support Scams. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*: 18-38; Chaganti, R., Bhushan, B., Nayyar, A. and Mourade, A. (2021). Recent Trends in Social Engineering Scams and Case Study of Gift Card Scam. arXiv preprint. arXiv:2110.06487; Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231.

7. Response to fraud

As a form of SOC, fraud is addressed by law enforcement. This relies on having adequate legislation in place as well as appropriate techniques to investigate and prosecute fraudsters who often engage in fraud internationally. This section explores the legal situation in Nigeria, Ghana and India, challenges with investigating and prosecuting fraud in the three countries, and the level of international collaboration.

7.1. Legal situation

All three countries have legislation in place to address fraud.

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 is the primary legislation targeting fraudsters in Nigeria. The Act is comprehensive in the types of cybercrime included, and it also places responsibility on financial institutions and service providers. Research indicates that the Cybercrimes Act has contributed significantly to the regulation and deterrence of several forms of cybercrime, including card and ATM fraud, Internet fraud, identity theft, malicious hacking, and data theft, hence safeguarding online businesses.[276]

The maximum penalty is seven years in prison, a fine of 7 million naira, or both, with varying charges depending on the type of cybercrime; but interviews reported that implementation is not stringent. Plea bargains are commonly applied, with the fine being no more than 10% of the money made; when released, fraudsters tell their peers how to negotiate the criminal justice system.[277] Mild punishments, with most suspects being given a 'slap on the wrists', means the legislation is not an effective deterrent.[278] The rate of reoffending is high.[279] However, the movement of Nigerian fraudsters to Ghana and other locations suggests some success in enforcement.

In 2020 Ghana introduced the Cybersecurity Act (Act 1038). However, the Act is procedural, setting out the establishment of the Cyber Security Authority and other mechanisms to promote cyber security. Legislation that targets fraudsters is set out in the Criminal Code 1960 (Act 27), the Electronic Transactions Act 2007 (Act 772) and the Economic and Organized Crime Act 2010 (Act 804). Ghana is also party to the Budapest Convention on Cybercrime and the African Union Malabo Convention on Cybercrime. Accordingly, the legal regime governing fraud is seen to be fragmented, spread across different regulations depending on the scope and nature of the offence.[280] This is seen as one of the drivers of Nigerian fraudsters' presence in Ghana.

In India there are two laws under which offenders can be prosecuted: the Information Technology Act (2000) and the Indian Penal Code (1860). The Information Technology Act provides protection against crimes such as email account hacking, credit card fraud, web defacement, virus introduction, phishing, and email scams.[281] However, critics argue that the existing Information Technology Act is outdated and does not cover the breadth of modern

---

[276] Idem, U. J. (2023). The Legal Approach for Fighting Cybercrimes in Nigeria: Some Lessons from the United States and the United Kingdom. *2023 International Conference On Cyber Management And Engineering (CyMaEn)*: 191–98.

[277] Interview with EFCC, Nigeria.

[278] Ekwenze, S. A. (2012). The Use of the Holy Bible, the Holy Qu'Ran, Juju and Others for Oath of Office: To Fight Corruption in Nigeria. *Law and Religion eJournal*.

[279] Interview with EFCC, Nigeria.

[280] Interview with law enforcement, Ghana.

[281] Dokku, S. R. and Kandula, D. (2021). A study on issues and challenges of information technology act 2000 in India. *Annals of Justice and Humanity* 1(1): 39–49. Available at: https://goodwoodpub.com/index.php/ajh/article/view/1389

cybercrime; the lack of legal procedural norms has prevented convictions when many cases are taken to court.[282] Trials take too long, sentencing is too lenient, and fraudsters get released on bail relatively easily.[283] For instance, the leader of a call centre in India spent 14 months in jail, compared to his conspirator, who was sentenced to 151 months in America.[284] Nevertheless, new regulations are coming into effect. The Indian government is making efforts to limit the distribution of SIM cards to registered companies only, with stronger approval processes. There are stronger 'Know your Customer' (KYC) requirements in banks, and there is more regulation by the central bank and financial regulators on the banking sector and stock exchange.[285]

A key challenge that emerges from legislation is that it focuses only on domestic crimes. This makes cross-border fraud more attractive, because it has less risk than national fraud. For example, although there are international regulations to prevent cold-calling in the USA, the UK and Europe, scammers do not respect do-not-call lists, and they take advantage of the fact that investigation, prosecution, extradition and compensation are difficult to do internationally.[286] Edwards et al. (2018) noted that:

> the exploitation of inter-state and international regulatory and criminal justice asymmetries – e.g. different levels of enforcement in the states or countries in which the fraudsters operate – represents a positive advantage for fraud compared with most other crimes.[287]

Although there is specific legislation to target fraud in each country, the reach of legislation differs. In addition, challenges arise in putting the legislation into practice. This is explored in the next section.

7.2. Investigating fraud

In all three countries, there is evidence that multiple agencies are now focused on fraud.

In Nigeria, the Office of the National Security Advisor (ONSA) coordinates the response to cybercrime, and the Cybercrime Advisory Council brings together all relevant ministries and agencies that respond to cybercrime. The EFCC is the key agency investigating cybercrime, prosecuting more than 3,000 fraudsters per year according to their website.[288]

The Nigeria Police Force (NPF) is actively engaged in combating cybercrimes through a specialised unit, the Cybercrime Unit, situated within the Force Criminal Investigation

---

[282] Interview with scamfighter, India; Vaidyanathan, R. (2020, 8 March). 'Confessions of a call-centre scammer'. Available at: https://www.bbc.com/news/stories-51753362

[283] Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea; Wen, N. J., Carolyn, M., Ang, J., Jingmin, H. and Shuyan, O. (2021). Uncovering the Workings of Credit-for-Sex Scams. Available at: https://www.mha.gov.sg/docs/hta_libraries/publications/07-crime.pdf; Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231.

[284] Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231.

[285] Interview with cyber expert, India; interview with law enforcement, India.

[286] Interview with fraudster, India; Harley, D., Grooten, M., Burn, S. and Johnston, C. (2012). My PC has 32,539 errors: how telephone support scams really work. Virus Bulletin; Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231; Tzani Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R. and Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. *Journal of Forensic and Investigative Accounting* 12(1): 163–78.

[287] Edwards, M., Suarez-Tangil, G., Peersman, C., Stringhini, G., Rashid, A. and Whitty, M. (2018, May). The geography of online dating fraud. Paper presented at Workshop on Technology and Consumer Protection, San Franciso, California, United States.

[288] https://www.efcc.gov.ng/

Departments in Abuja and Alagbon, Lagos.[289] The NPF has also established a dedicated cybercrime complaint reporting website, enabling individuals to report experiences of victimisation.[290]

In recent years, Ghana has pledged to increase efforts to tackle transborder crime, including cyber fraud.[291] The Cybersecurity Act (2020) established the Cyber Security Authority to regulate cybersecurity and promote the development of cybersecurity within Ghana. The Ghana Police Service has a cybercrime unit that pursues cybercrime cases, although this is seen to be a low priority compared to other crime types.[292] The Ministry of National Security has the National Signals Bureau, which provides secure systems for national security and intelligence agencies, and the Bureau of National Investigations, which focuses on organised and financial crime. In addition, the Economic and Organised Crime Office (EOCO) has a cybersecurity centre and a WhatsApp hotline for reporting cases. The challenge with having multiple agencies involved is the risk of turf wars, although there are indications of cooperation.[293]

In India, the Central Bureau of Investigation (CBI) supports on intelligence but the actual case and prosecution work is done by state police.[294] The growing prevalence of cybercrime has led to increased police technical training and the creation of dedicated cyber cells. National law enforcement has been successful in shutting down major cross-border fraud centres. [295] In some cases this was done with international support; this is discussed in more detail below. At the national level, a source claims that Indian law enforcement focuses on fraud that targets domestic victims.[296]

7.2.1. Challenges in investigation

Despite the commitment of multiple agencies to tackle fraud, there are specific challenges that arise from investigating fraud, especially cyber-enabled fraud. The approach to investigate and prosecute cybercrimes differs from that for other forms of crime. Law enforcement has fewer tools to gather evidence, and there is a heavy reliance on testimony.[297] In addition, the way investigators see cybercrime offences is seen to be out of alignment with the legal system.[298] Scammers are also constantly innovating their tactics to remain ahead of law enforcement and security measures (see Section 3.8).

Additional challenges emerge with regard to identifying fraud and fraudsters. Cybercrime leaves imperceptible traces that demand advanced expertise to identify, evaluate the evidential value

---

[289] Ismail, U. (2020). The Nigeria Police Force and Cybercrime Policing: An Appraisal. *Dutse Journal of Criminology and Security Studies* 4(1): 78–88.

[290] Ismail, U. (2020). The Nigeria Police Force and Cybercrime Policing: An Appraisal. *Dutse Journal of Criminology and Security Studies* 4(1): 78–88.

[291] Adebayo, B. (2023, 15 August). 'Sakawa Boys: Meet Ghana's online romance scammers'. Available at: https://www.context.news/digital-rights/sakawa-boys-meet-ghanas-online-romance-scammers

[292] Interview with law enforcement, Ghana.

[293] Interview with law enforcement, Ghana.

[294] Interview with law enforcement, India.

[295] Wen, N. J., Carolyn, M., Ang, J., Jingmin, H. and Shuyan, O. (2021). Uncovering the Workings of Credit-for-Sex Scams. Available at: https://www.mha.gov.sg/docs/hta_libraries/publications/07-crime.pdf; Nilsson, M. G; Lester, D; Pylarinou, N. R; & Ioannou, M. (2020). Profiling HMRC and IRS scammers by utilizing trolling videos: Offender characteristics. Journal of Forensic and Investigative Accounting, 12(1), 163–78; Microsoft (2021). Global Tech Support Scam Research. Available at: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2021/07/MSFT-2021-Global-Tech-Support-Scam-Research-Report.pdf; interview with law enforcement, India.

[296] Interview with law enforcement, India.

[297] Interview with EFCC, Nigeria.

[298] Interview with EFCC, Nigeria.

of, and capture the diverse evidence discovered in a digital forensic investigation.[299] The difficulties are compounded by the need to grapple with the malleable nature of various storage media, including storage peripherals, electronic components, working memory, hard discs, and external discs.[300] A key challenge for investigation is that one person can be engaged in multiple fraud with different identities.[301] In Nigeria there are reports of inappropriate investigation techniques being applied to cases, including arbitrary arrests, freezing of bank accounts, intimidation, harassment, and seizure and search of digital devices and cyberspace applications. Nigerian youth have protested against these investigation techniques.[302] Despite this, there is also evidence that Nigerian law enforcement have developed extensive expertise on cybercrime and are well informed about the many techniques used by yahoo boys to deceive victims.[303] As a result, many fraudsters are being brought to justice.[304] The approach is primarily responsive, driven by cases, rather than proactive.[305]

In Ghana one interviewee questioned the effectiveness of law enforcement, given there are houses that are not raided but are widely known to contain multiple fraudsters.[306] There have also been cases of frauds being conducted from within prison. This is echoed in the literature, with one article highlighting that "traditional policing strategies remains repressive and reactive and are unable to control Sakawa-related activities effectively in the country", and another stating:[307]

> A prisoner in Ghana's Ankaful Maximum Security Prison used a smuggled mobile phone to organize a mobile money fraud scheme with the help of accomplices. A lawyer uncovered the inmate's identity and continued communicating with him and another prisoner pretending to be interested in a business partnership.[308]

In India, scammers operate across state borders as part of a large, decentralised network (see Section 4.3), and because investigations are done by state police without much cross-border collaboration, it becomes difficult to connect the dots and work collaboratively. Scammers use new SIM cards and disposable mobile devices and constantly shift base to avoid detection.[309] There are reports of centres removing all evidence and data by the time the police conduct a raid, disguising themselves as legitimate call centres ('in plain sight'), being located in buildings hidden from public view or requiring fingerprint scanning to enter.[310] Even if police freeze bank

---

[299] Arewa, A. (2018). Borderless crimes and digital forensic: Nigerian perspectives. *Journal of Financial Crime* 25(2): 619–31.

[300] Ibid.

[301] Interview with scamfighter.

[302] Richards, N. U. and Eboibi, F. E. (2023). Cybercrime perspectives to the 'ENDSARS' protest in Nigeria. *African Security Review* 32(1): 38–56.

[303] Adejoh, S. O., Alabi, T. A., Adisa, W. B. and Emezie, N. M. (2019). "Yahoo Boys" Phenomenon in Lagos Metropolis: A Qualitative Investigation. *International Journal of Cyber Criminology* 13(1):1–20.

[304] Interview with HMG.

[305] Interview with scamfighter.

[306] Interview with government, Ghana.

[307] Akuako, E. (2022). The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana. Available at: https://dr.library.brocku.ca/handle/10464/16385

[308] Arthur-Mensah, G. (2023, 4 September). 'Ghana records GH¢49.5m Ghana Cedis losses through cyber fraud in first half of 2023'. Available at: https://gna.org.gh/2023/09/ghana-records-gh¢49-5m-losses-through-cyber-fraud-in-first-half-of-2023/

[309] Interview with cyber expert, India; Tzani Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R. and Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. *Journal of Forensic and Investigative Accounting* 12(1): 163–78; Microsoft (2021). Global Tech Support Scam Research. Available at: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2021/07/MSFT-2021-Global-Tech-Support-Scam-Research-Report.pdf; interview with fraudster, India.

[310] Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea;

accounts within 24 hours of getting a complaint, money is routed to other accounts, and bank documents contain fake information.[311] The methods used by scammers to escape detection when moving proceeds have been explored in Section 6. The police also face issues such as delays in getting approval, lack of funding and technology, and lack of training.[312]

Other issues include the fact that Indian fraudsters usually steal small sums from individual victims, and so the crime goes underreported around 60% of the time. This challenge is compounded by the fact that victims are often unaware of where the scammer is calling from.[313] Even technical solutions to cyberattacks, such as phishing detection software, do not address the human aspect of social engineering.[314] As a result, there does not seem to have been a conspicuously effective impact on the problem so far. Despite successful raids and arrests, the number of prosecutions has been minimal compared to the number of phone calls that continue.[315]

A more severe criticism from some sources is that the Indian police are largely ineffective, slow and inefficient, and lack the will and ability to respond seriously to threats.[316] For example, the online cybercrime portal did not accept forms if the complainant did not have an Indian number, making it impossible for foreigners to report a crime.[317]

7.2.2. Displacement

Fraudsters are agile and innovative. For example, if a fraudulent website is identified and taken down, they will move to another site immediately.[318] There is also only limited cooperation from website providers. For example, in one Nigerian case, in which the website of a legitimate business was being spoofed, the site was reported to the host, GoDaddy, which registered the case but took no action.[319]

In India, despite efforts by governments, law enforcement, scamfighters and private companies, scam operations scatter and re-emerge even after being shut down, as they are quick to evolve their methods.[320] A former fraudster is quoted as saying, "Even if you shut down 400 buildings in

---

Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231.

[311] Vaidyanathan, R. (2020, 8 March). 'Confessions of a call-centre scammer'. Available at: https://www.bbc.com/news/stories-51753362

[312] Interview with cyber expert, India; Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231.

[313] Harley, D., Grooten, M., Burn, S. and Johnston, C. (2012). My PC has 32,539 errors: how telephone support scams really work. Virus Bulletin; Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231.

[314] Liu, J., Pun, P., Vadrevu, P. and Perdisci, R. (2023). Understanding, Measuring, and Detecting Modern Technical Support Scams. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*: 18-38; Chaganti, R., Bhushan, B., Nayyar, A. and Mourade, A. (2021). Recent Trends in Social Engineering Scams and Case Study of Gift Card Scam. arXiv preprint. arXiv:2110.06487.

[315] Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231.

[316] Interview with scamfighter, India; Vaidyanathan, R. (2020, 8 March). 'Confessions of a call-centre scammer'. Available at: https://www.bbc.com/news/stories-51753362; interview with journalist, India; Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea

[317] Interview with scamfighter, India.

[318] Interview with scamfighter.

[319] Interview with scamfighter.

[320] Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0; interview with law enforcement, India; Microsoft (2021). Global Tech Support Scam Research. Available at: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2021/07/MSFT-2021-Global-Tech-Support-Scam-Research-Report.pdf

India, it will not stop".[321] As mentioned previously, there are now more small-scale centres after law enforcement cracked down on bigger ones. Although there are some arrests, the people at the top are rarely caught, and hence they can quickly recover and relocate.[322] For example, the IRS scheme started in Gujarat but has now shifted to Bangalore, Delhi, Gurgaon and other cities after the FBI got involved.[323] Displacement can also occur internationally. For instance, some academic literature has found that in Spain, police interest in organised fraud has been low and there are more opportunities for scammers to conceal their activities.[324]

7.2.3. Judicial understandings of fraud

When investigations are taken forward, further challenges arise in court. Judges do not have a good understanding of the architecture of online fraud and what constitutes evidence.[325] Although law enforcement has undergone training to strengthen the approach to cyber frauds, this has not extended to the judiciary.[326]

A study conducted by Mohammed et al. (2019) that focused on Nigerian fraud emphasises the growing significance of digital evidence in both criminal and civil courts, highlighting the need for judges to have a general understanding of the underlying technologies and applications from which digital evidence is derived.[327]

India also faces major barriers in obtaining convictions. The police may arrest perpetrators, but they are unable to obtain convictions in court, because of issues such as admissibility of evidence. [328] A scamfighter explained how they gave a tip about the location of a call centre but there were no arrests after the police conducted a raid, as they required hard evidence of money being stolen.[329] A police investigator stated, "As multiple parties are involved […] it's difficult to get full information and complete the chain of events. [The facilitators] who are in foreign jurisdictions do not provide all the information required for prosecution".[330] The victims are often based abroad and do not give depositions which are demanded by the court, as per the Evidence Act in the Indian Penal Code.[331]

---

[321] Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0

[322] Interview with scamfighter, India; interview with fraudster, India; interview with journalist, India; Harley, D., Grooten, M., Burn, S. and Johnston, C. (2012). My PC has 32,539 errors: how telephone support scams really work. Virus Bulletin; Microsoft (2021). Global Tech Support Scam Research. Available at: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2021/07/MSFT-2021-Global-Tech-Support-Scam-Research-Report.pdf

[323] Interview with fraudster, India.

[324] Tzani Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R. and Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. *Journal of Forensic and Investigative Accounting* 12(1): 163–78; Levi, M. (2014). Organized fraud. In Paoli, L. The Oxford Handbook of Organized Crime. Oxford: Oxford University Press; Button, M., Nicholls, C. M., Kerr, J. and Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology* 47(3): 391–408. doi: 10.1177/0004865814521224.

[325] Interview with law enforcement, Ghana; interview with law enforcement, Ghana.

[326] Interview with law enforcement, Ghana.

[327] Mohammed, K. H., Mohammed, Y. D. and Solanke, A. A. (2019). Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime* 2(1): 56–63.

[328] Interview with journalist, India; interview with scamfighter, India; interview with law enforcement, India.

[329] Interview with scamfighter, India.

[330] Interview with law enforcement, India.

[331] Ally, A. J. and Gadgala, N. (2022). Addressing Cyber Scam as a Threat to Cyber Security in India. *International Journal of Law Management & Humanities* 5(3): 376–90; Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea; interview with law enforcement, India.

7.2.4. Corruption

Corruption is a major barrier to investigation. In Nigeria there are reports that the Black Axe confraternity has judges on the payroll.[332] Similarly, the leaders of Nigerian fraud groups are perceived to have contacts within law enforcement who warn them if they are being investigated.[333] There is also evidence of close connections of some Black Axe leaders to senior politicians in Nigeria. Even without insiders, the revenue being made through fraud ensures that fraudsters can offer 'dash' and 'gratification'[334] to investigators and can afford the best legal representation, which has resulted in many adjournments in court.[335]

Corruption is also a problem in Ghana, with some law enforcement officers colluding with fraudsters to evade the law.[336] One fraudster interviewed was arrested but released without charge after he bribed officers with 4000 cedi (230 GBP).[337] If police refuse to accept bribes, there are cases in which fraudsters have identified others, such as the officer's medical doctor, who can influence the police officer to pressure the police.[338] Fraudsters also leverage linkages with politicians to pressure police to drop their case, which makes it dangerous to pursue these kinds of cases.[339]

Some scam centres in India enjoy patronage from local police and politicians, who collect 'cuts' of what is stolen, which means centres can get off easily if arrested.[340] It is argued that this patronage is small-scale and at the local level, especially as corruption reduced when the USA and central authorities got more involved.[341] Social media has also undermined this, as victims report fraud on online platforms and gain public attention, prompting police responses and, potentially, reducing corruption and inertia.[342]

These challenges within Nigeria, Ghana and India highlight the importance of international collaboration.

7.3. International collaboration

Frauds are not necessarily contained within a country, so international collaboration is required. There is evidence of collaboration between law enforcement agencies in one country and their counterparts in other countries. Increasingly, other actors are also becoming involved, including the private sector and scamfighters.

In Nigeria, international collaboration works in both directions – when Nigerian investigators are exploring the targets of Nigerian fraudsters and when law enforcement in other countries trace frauds back to Nigeria.[343] Key partners include the USA's FBI, the Canadian Police and the Australian Police, with some cooperation with the Metropolitan Police in the UK.[344] However,

---

[332] Interview with scamfighter.

[333] Interview with scamfighter.

[334] 'Dash' and 'gratification' refer to bribes or facilitation payments.

[335] Interview with EFCC, Nigeria; interview with fraudster, Nigeria.

[336] Interview with law enforcement, Ghana.

[337] Interview with fraudster, Ghana.

[338] Interview with law enforcement, Ghana.

[339] Interview with an academic, Ghana.

[340] Interview with cyber expert, India; interview with fraudster, India; interview with journalist, India; interview with scamfighter, India.

[341] Interview with law enforcement, India; interview with law enforcement, India; interview with fraudster, India.

[342] Interview with journalist, India.

[343] Interview with EFCC, Nigeria.

[344] Interview with EFCC, Nigeria; interview with EFCC, Nigeria.

gaps emerge in relation to countries where there is no cooperation treaty in place, for example when monies are traced to Hungary or China.[345] This is also understood by fraud networks: many BEC cases use Hungarian accounts because they know the money will not be easy to trace.[346]

Ghana frequently collaborates with the FBI, and the FBI has conducted training for security officers and has provided software and information communication technology tools to extract information.[347] There is also collaboration with the UK through the National Crime Agency (NCA), as well as with India, France, Germany, Canada and the European Union.[348]

India has also received cooperation on specific cases from law enforcement abroad. IRS and tech support scams targeting Americans saw a significant reduction after the FBI got involved and shut down call centres in several high-profile cases.[349] With the support of the British police and Microsoft, a call centre in Kolkata defrauding thousands of people in the UK was shut down by the local police.[350] These disruption efforts have impacted the industry, and the scale of organisation is significantly reduced; call centres are now more scattered across the country and of smaller scale, but are still numerous.[351] There are other examples of the success of international cooperation; for instance, in 2023 the CBI launched Operation Chakra-II (see box below). However, there is scope for better cross-border relationships between governments and law enforcement agencies.[352] The USA is seen to be the most involved and effective in both investigation and prosecution of cases originating in India.[353] In contrast, there is less of a common response across Europe, for instance.[354]

There is also a private sector response to fraud. Multinational companies such as Microsoft and Amazon have fraud teams that investigate and report call centre scams that impersonate them, and they collaborate with governments and law enforcement, leading to some successful raids.[355] Another emerging group are Internet vigilantes, known as 'Scamfighters', who impersonate victims to disrupt operations, often garnering millions of views on YouTube and other social media, thereby also raising awareness. They employ tactics such as hacking into scammers' computers, deleting files, shutting down networks, and reporting their locations to law enforcement. They have an advantage that tech companies and law enforcement do not,

---

[345] Interview with EFCC, Nigeria.

[346] Interview with EFCC, Nigeria.

[347] Interview with law enforcement, Ghana; interview with law enforcement, Ghana.

[348] Interview with law enforcement, Ghana; interview with government, Ghana.

[349] Interview with fraudster, India; interview with fraudster, India; interview with law enforcement, India; Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0

[350] Dhankar, L. (2023, 2 March). 'Two foreigners held in call centre fraud were planning to flee India, say police'. Available at: https://www.hindustantimes.com/cities/gurugram-news/two-foreigners-held-in-call-centre-fraud-were-planning-to-flee-india-say-police-101677776845652.html

[351] Interview with fraudster, India; interview with scamfighter, India.

[352] Interview with law enforcement, India; Harley, D., Grooten, M., Burn, S. and Johnston, C. (2012). My PC has 32,539 errors: how telephone support scams really work. Virus Bulletin; Mathai, A. (2022). 'Ever lost money to digital fraudsters? Join the club'. Available at: https://www.theweek.in/theweek/specials/2022/06/24/ever-lost-money-to-digital-fraudsters-join-the-club.html; Johnson, B. M. (2022, 10 April). 'Rise of the scam baiter - fall of the scammers'. Available at: https://www.linkedin.com/pulse/rise-scam-baiter-fall-scammers-bronwyn-may-johnson-mba-/

[353] Interview with cyber expert, India; interview with journalist, India.

[354] Interview with cyber expert, India.

[355] Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea; Dhankar, L. (2023, 2 March). 'Two foreigners held in call centre fraud were planning to flee India, say police'. Available at: https://www.hindustantimes.com/cities/gurugram-news/two-foreigners-held-in-call-centre-fraud-were-planning-to-flee-india-say-police-101677776845652.html

which is being able to use illegal techniques such as hacking, and their work has exposed hundreds of scammers. [356]

Although the investigation and prosecution of fraud has improved in Nigeria, Ghana and India, including through international collaboration, there is a need for constant evolution, in line with the tactics of fraudsters. In all three countries the USA has been the most active international partner, with less engagement with the UK.

Operation Chakra-II

The CBI has launched Operation Chakra-II to fight against transnational organised cyber-enabled financial crimes in India. For this, India's federal agency has partnered with Microsoft and Amazon as well as with national and international agencies to combat and dismantle infrastructure of illegal call centres.[357] The CBI is working with the FBI, INTERPOL's Cyber Crime Directorate and the INTERPOL Financial Crime and Anti-Corruption Centre, the NCA in the UK, Singapore Police Force and the Federal Criminal Police Office of Germany to notify further leads. Under Operation Chakra, launched last year, the CBI conducted raids over 100 locations against cyber criminals involved in financial crimes.

[356] Liu, J., Pun, P., Vadrevu, P. and Perdisci, R. (2023). Understanding, Measuring, and Detecting Modern Technical Support Scams. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*: 18-38; Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea; Harley, D., Grooten, M., Burn, S. and Johnston, C. (2012). My PC has 32,539 errors: how telephone support scams really work. Virus Bulletin; RNZ (2018, 14 January). 'The desperation of India's scammers'. Available at: https://www.rnz.co.nz/national/programmes/up-this-way/audio/2018628439/the-desperation-of-india-s-scammers; interview with scamfighter, India.

[357] Times of India (2023, 20 October). 'CBI launches Operation Chakra-II: What it is and why Microsoft and Amazon are part of this'. Available at: https://timesofindia.indiatimes.com/gadgets-news/cbi-launches-operation-chakra-ii-what-it-is-and-why-microsoft-and-amazon-are-part-of-this/articleshow/104582380.cms

8. Perceptions of fraud

The response to fraud is also influenced by how it is perceived. This section explores political perceptions and the political will to address fraud, as well as the wider public perception. Linked to motivations, the research also identified strategies employed by fraudsters to justify their activities.

8.1. Political perceptions

Political perceptions tend to be influenced by the impact fraud has on political actors. In Nigeria, cyberfraud does not garner significant political attention. Many politicians believe it tarnishes their image, so they prefer to avoid engaging with the issue.[358] Other politicians are linked to frauds or laundering the proceeds, and do not want to draw attention or do not view it as criminal.[359]

In Ghana, cyber fraud has become more of a politically salient issue because politicians have been victims of fraud. One interviewee noted:

> There have been a number of politicians whose Facebook accounts were duplicated, and then you have others who are impersonating them as being them on Facebook. […] So you would see that the politician themselves have become victims, and they are not happy.[360]

As a result, there has been increased political attention to strengthen the response, including establishing the National Cybersecurity Authority. This is seen as an indication that the political class are serious about tackling cybercrime.[361]

However, others are less convinced. Another interviewee highlighted that some of the fraudsters are related to party executives.[362] In addition, "politicians also want money, so if they are able to solve the problem for the suspect or the criminal, they will get money to fund their political activities".[363] Revenue also comes into the country from the cars purchased by fraudsters, as many are imported, with large duties paid on them.[364]

Although some call centres in India have political patronage (see Section 7.2), politicians are not overtly supportive of fraud. There is some indication of fraud being part of the policy agenda for the Government of India. For instance, UNODC and the Ministry of Home Affairs co-led a three-day conference on cybercrime during the G20 Summit in 2023, acknowledging the need to address threats such as ransomware, phishing, online scams and hacking. Proposed solutions included robust cyber security mechanisms and cooperation and information sharing.[365]

---

[358] Interview with EFCC, Nigeria.

[359] Interview with EFCC, Nigeria.

[360] Interview with law enforcement, Ghana.

[361] Interview with law enforcement, Ghana.

[362] Interview with law enforcement, Ghana.

[363] Interview with law enforcement, Ghana.

[364] Interview with government, Ghana.

[365] UNODC (2023). 'India: UNODC Joins Forces with India's Ministry of Home Affairs for the G20 Conference on Cyber Security'. Available at: https://www.unodc.org/southasia//frontpage/2023/July/india_-unodc-joins-forces-with-indias-ministry-of-home-affairs-for-the-g20-conference-on-cyber-security.html

8.2. Public perceptions

The public perception of fraud is also mixed, with an evident generational divide. For example, in Nigeria older generations see fraud as a bad thing, but younger generations see it as a positive.[366] There are also differences in perception between north and south. Across Southern Nigeria, those involved in fraud do not attempt to hide it; they drive expensive cars and spend money entertaining.[367] In the North, if someone were involved in fraud they would be discreet, because it would not be viewed positively.[368]

A concerning trend is emerging among parents of fraudsters in Nigeria. Not all parents are aware of the involvement of their children, but there is a growing cohort of parents who support the fraudulent activities of their children.[369] Interviewees reported on the emergence of associations of mothers of yahoo boys that meet to discuss how to provide support for their children and increase their earnings.[370] Some parents even procure laptops and phones to be used in fraud schemes, and others take their children to academies to learn how to become a fraudster.[371] A study that interviewed 52 parents of fraudsters found a tendency among parents to neutralise the behaviour of their children, excusing themselves from societal norms.[372] This undermines the role of the family in controlling deviant behaviour.[373]

The prevalence of cyber fraud is less normalised in Ghana. One interviewee noted:

> I would be so bold as to say almost every young Nigerian in the country at least knows someone who's into cybercrime. […] That is how widespread it is. In Ghana it is not so. Though scam networks seem to be gaining ground, it is still a way of life considered foreign and greatly frowned upon by majority of the country's population.[374]

Although fraudsters are seen as flashy, and generally people who live flamboyantly are revered, they are often recognised as people to avoid and are seen as a social menace.[375] However, for some, including young people, this flashy behaviour is something to emulate, and they become role models – at least until they are caught.[376] There are schools emerging that teach cyber fraud techniques in Ghana, and there are cases of parents bringing their children to learn.[377]

As discussed in Section 5, the perception of fraud is mixed among fraudsters in India themselves. Some feel guilt and justify it as a means to an income. Others may glorify the job and take pride in stealing money, particularly because of the glamour and lifestyle that come with the role. Among larger society, however, interviews conducted for this study reveal that there is a low social acceptance for fraud and crimes in general, with very few people agreeing with the 'Robin

---

[366] Interview with fraudster, Nigeria.

[367] Interview with prison officer, Nigeria.

[368] Interview with prison officer, Nigeria.

[369] Aborisade, R. A. (2022). Yahoo Boys, Yahoo Parents? An Explorative and Qualitative Study of Parents' Disposition towards Children's Involvement in Cybercrimes. *Deviant Behavior* 44(7): 1102–20.

[370] Interview with NGO, Nigeria.

[371] Interview with NGO, Nigeria.

[372] Aborisade, R. A. (2022). Internet Scamming and the Techniques of Neutralization: Parents' Excuses and Justifications for Children's Involvement in Online Dating Fraud in Nigeria. *International Annals of Criminology* 60(2): 199–219.

[373] Ibid.

[374] Interview with scamfighter.

[375] Interview with government, Ghana; interview with law enforcement, Ghana; interview with law enforcement, Ghana; interview with law enforcement, Ghana; interview with law enforcement, Ghana.

[376] Interview with law enforcement, Ghana.

[377] Interview with law enforcement, Ghana.

Hood' line of thinking. Instead, fake call centres are considered a 'blight' which is tarnishing India's reputation.[378] This becomes more apparent when looking at case studies of individual fraudsters, most of whom do not tell their parents and family the true nature of their job, but instead claim to be working at a legitimate call centre. Parents often express shock and disappointment when their children are arrested.[379] It is also worth noting that some pockets of the country have become scam hubs, and most people in the village or town are complicit (also discussed in Section 5). There is higher acceptance in these areas because the industry is bringing jobs, wealth and investment.[380]

8.3. Strategies to rationalise fraud

Those involved in fraud have developed strategies to justify their activities.

In both Nigeria and Ghana, strategies have been developed to reframe cyberfraud in a positive light, although these techniques to neutralise perspectives are stronger in Nigeria. As mentioned above, there are narratives in Nigeria that fraudsters are repatriating stolen artefacts and wealth.[381] One study identified:

> [a] widespread belief among ordinary individuals that acquiring wealth and influence necessitates resorting to deception and corruption. Observers attribute this perception to a historical and cultural connection with the revered trickster, colloquially known as 'the feyman'. This figure is depicted as a cunning individual who not only engages in trickery but also harnesses the powers of magic and witchcraft.[382]

Similar narratives are taking hold in Ghana.[383] An investigation by the Australian Broadcasting Corporation (ABC) interviewed fraudsters in Accra Internet cafes, with one stating:

> It might be somehow painful seeing someone who is old enough to be your mother going through that, but the bottom line still remains, we've got to survive. The white people, they came down here to colonise us, took what belongs to us. They sent our great-great-grandfathers there, mistreated them, treated them like slaves, they did a lot of harm to them. They've done us bad before and we think it's time to pay them back.[384]

A study of comments shared in relation to cybercrime by Ghanaian Facebook users found these views are becoming more widely held, with commenters associating fraud with an opportunity to "push back against Western dominance", as well as internal politics and financial insecurity.[385]

---

[378] Interview with cyber expert, India; interview with law enforcement, India; interview with journalist, India.

[379] Interview with cyber expert, India; interview with journalist, India; interview with law enforcement, India; interview with law enforcement, India; Microsoft (2021). Global Tech Support Scam Research. Available at: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2021/07/MSFT-2021-Global-Tech-Support-Scam-Research-Report.pdf

[380] Interview with cyber expert, India.

[381] Interview with EFCC, Nigeria; interview with EFCC, Nigeria; interview with NGO, Nigeria; interview with EFCC, Nigeria.

[382] Glickman, H. (2005). The Nigerian "419" Advance Fee Scams: Prank or Peril? *Canadian Journal of African Studies* 39(3): 460–89.

[383] Rubinsztein-Dunlop, S., Robinson, L. and Dredge, S. (2019). 'Meet the scammers: Could this be your online lover?' Available at: https://www.abc.net.au/news/2019-02-11/ghana-meet-the-scammers/10785676; Abubakari, Y. and Blaszczyk, M. (2023). Politicization of Economic Cybercrime: Perceptions Among Ghanaian Facebook Users. *Deviant Behavior* 45(4): 483–502; Barnor, J. N. B., Boateng, R., Kolog, E. A. and Afful-Dadzie, A. (2020). Rationalizing online romance fraud: In the eyes of the offender. *AMCIS 2020 Proceedings*. 21. Available at: https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/21

[384] Rubinsztein-Dunlop, S., Robinson, L. and Dredge, S. (2019). 'Meet the scammers: Could this be your online lover?' Available at: https://www.abc.net.au/news/2019-02-11/ghana-meet-the-scammers/10785676

[385] Abubakari, Y. & Blaszczyk, M. (2023). Politicization of Economic Cybercrime: Perceptions Among Ghanaian Facebook Users. *Deviant Behavior* 45(4): 483–502.

Other strategies to neutralise fraud in Ghana include believing that victims are wealthy and do not lose anything when they are scammed, and distinguishing fraud from traditional criminal activities, such as robbery or murder, to present it as a less heinous crime.[386]

Endemic corruption within Nigeria is also used to justify fraud:[387]

> A respondent in a survey seeking parents' perspectives on Nigerian cybercrime expressed: "If a 419 boy [cybercriminal] is arrested, people would be sympathetic to him. They would ask, 'What type of crime has he committed? Is it just because he defrauded someone? Is it bigger than the ones people in government are committing? Why are they treating the small boy [cybercriminal] as if he has done something terrible?'"[388]

A study of Nigerian hip-hop identified 33 songs that justify the fraudulent actions of online fraudsters, blame and dehumanise victims of online romance fraud, and glamorise online fraud. The study provided insights into prevailing attitudes, Indigenous linguistics, and world views with regard to cybercrime victimisation.[389] Similarly, the Ghanaian film industry has been seen to contribute to the rationalisation of Sakawa – increasing its acceptance and the glamorisation of cybercrime.[390]

In India, as discussed in Section 5.2, some fraudsters experience guilt and remorse. These fraudsters tend to adjust their strategies, such as only targeting foreign nationals, rather than developing narratives that justify or rationalise their activity.

In all countries there is some recognition among all actors – politicians, the wider public, and those engaged in fraud – that it is an exploitative act.

---

[386] Barnor, J. N. B., Boateng, R., Kolog, E. A. and Afful-Dadzie, A. (2020). Rationalizing online romance fraud: In the eyes of the offender. *AMCIS 2020 Proceedings*. 21. Available at: https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/21

[387] Ibrahim, S. (2016). Causes of Socioeconomic Cybercrime in Nigeria. In International Conference on Cybercrime and Computer Forensic (ICCCF): 1–9; Okpe, V. V. and Taya, S. L. (2018). Political Perspective: Evaluating the Causes of Cybercrime in Nigeria. *Asian Journal of Multidisciplinary Studies* 6(12): 42–52; Ribic, P. (2019). The Nigerian email scam novel. *Journal of Postcolonial Writing* 55(3): 424–36.

[388] Ibrahim, S. (2016). Causes of Socioeconomic Cybercrime in Nigeria. In International Conference on Cybercrime and Computer Forensic (ICCCF): 1–9.

[389] Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T. and Okolorie, G. U. (2023). Cheques or dating scams? Online fraud themes in hip-hop songs across popular music apps. *Journal of Economic Criminology* 2: 100033.

[390] Oduro-Frimpong, J. (2014). Sakawa rituals and cyberfraud in Ghanaian popular video movies. *African Studies Review* 57(2): 131–47.

9. Emerging trends

Fraud is evolving fast in Ghana and Nigeria, with improvements in technology in particular. In contrast, fraudulent call centres in India continue to use unsophisticated technology. Another trend that has emerged in West Africa is reliance on juju, or spiritualism, which is believed to enhance the effectiveness of scams, particularly those that rely on social engineering.

9.1. Technology

Frauds already capitalise on technology to scam victims, but there is evidence of fraudsters engaging with emerging technology to improve their tactics. For example, financial transactions make use of cryptocurrency, which creates challenges for traceability.[391] VPNs are also used to disguise the location of the fraudster.[392] There are applications being used to enhance social engineering, such as converting the voice of the fraudster to a British accent.[393] AI is making these changes even smoother: it can change the language, the background and the image of the fraudster.[394]

One interview highlighted the extent to which Nigerian fraud networks would go in using technology to dupe victims, referring to a network with a fake banking system:

> It can be that it looks nice in the front, that it looks authentic. Then let's take to the back is a whole pseudo banking system, basically a database where you can actually show certain amounts in the account, etc.[395]

Ghanaian fraudsters are not seen to have the same technological skills as fraudsters from other countries, including Nigeria, such as being able to hack into systems.[396] However, many fraudsters are using technology to improve their activities. One interviewee noted that many fraudsters are IT specialists or are trained by IT specialists, so they use VPNs and use modern laptops.[397] AI is used to change the voice and image of the fraudster[398] and is also used to make fake statements and naked pictures that can be used for blackmail.[399] The dark web is used for training, accessing software and technology, such as that required to clone bank cards.[400]

In contrast, fraudulent call centres in India reportedly do not use sophisticated technology, as discussed in Section 3. Tools used include SIM cards, Voice over Internet Protocol (VoIP) – which allows them to make phone calls over the Internet – fake email IDs, VPNs, support domains, and fake websites to conduct phone and Internet scams.[401] There is no evidence to indicate that

---

[391] Interview with EFCC, Nigeria.

[392] Interview with fraudster, Nigeria; interview with ex-fraudster, Nigeria; interview with prison officer, Nigeria.

[393] Interview with NGO, Nigeria.

[394] Interview with scamfighter; interview with NGO, Nigeria.

[395] Interview with scamfighter.

[396] Interview with law enforcement, Ghana.

[397] Interview with government, Ghana.

[398] Interview with law enforcement, Ghana; interview with law enforcement, Ghana; interview with law enforcement, Ghana; interview with government, Ghana.

[399] Interview with politician, Ghana.

[400] Interview with politician, Ghana.

[401] Interview with cyber expert, India; interview with fraudster, India; interview with fraudster, India; interview with journalist, India; interview with law enforcement, India; interview with law enforcement, India; Wen, N. J., Carolyn, M., Ang, J., Jingmin, H. and Shuyan, O. (2021). Uncovering the Workings of Credit-for-Sex Scams. Available at: https://www.mha.gov.sg/docs/hta_libraries/publications/07-crime.pdf; Srinivasan, B., Kountouras, A., Miramirkhani, N., Alam, M., Nikiforakis, N., Antonakakis, M. and Ahamad, M. (2018, April). Exposing search and advertisement abuse tactics and infrastructure of technical support scammers. *WWW '18: Proceedings of the 2018 World Wide Web Conference*: 319–28.

fraudsters use voice-changing technology; most legitimate call centres are outsourced and hence Indian accents are acceptable, especially due to the reliance on social engineering.[402] An interview with a cyber expert revealed that AI is being used to generate fake profiles, images and scripts.[403] Less is known about how technology is used in new and emerging forms of fraud that target Indian and foreign victims, such as cryptocurrency fraud.

9.2. Spirituality

In both Ghana and Nigeria spirituality, or juju, is being used to enhance frauds, maximise income and prevent arrests.[404] Criminals employing juju do so to ensure their invincibility, avoid harm or death, subdue victims and elude police apprehension, and they engage with juju because they believe it is effective.[405]

Research confirms a widespread belief in the power and effectiveness of juju rituals in Nigeria, even among individuals affiliated with orthodox religions.[406] Because of the increasing awareness of scams globally, some fraudsters now believe that the 'reality of the hustle' means that "without adding some form of spiritual assistance or 'jazz' (voodoo), it is challenging to succeed in scamming clients".[407]

In Nigeria, the use of juju to improve fraud is referred to as 'yahoo plus' or going 'diabolical'. A survey of 800 students in secondary and tertiary institutions in Delta State on the prevalence of yahoo plus revealed that engaging in inhuman ritual activities for wealth creation has reached alarming levels, particularly in Delta State.[408] The report highlighted widespread instances of missing female university undergraduates and other school-aged girls being used for yahoo plus money rituals.[409] For example, in one extreme case, four teenage boys were arrested in Ogun State in February 2022 for murdering the girlfriend of one of the boys, cutting her head off and burning it in a pot.[410] In other cases, charms are prepared under the instruction of juju priests, with different animals, roots and herbs, but these charms require the blood of children or young women to maintain them.[411] The aim of the charms is to hypnotise victims so that whatever the fraudster says, they will comply.[412] However, there is a division between those that engage in yahoo yahoo and those that engage in yahoo plus.

---

[402] Interview with fraudster, India.

[403] Interview with cyber expert, India.

[404] Interview with NGO, Nigeria; interview with NGO, Nigeria.

[405] Aborisade, R. A. and Adedayo, S. S. (2021). 'Catch me if you can': the myth and reality of criminals' use of juju to evade arrest from the Nigeria police. *Police Practice and Research* 22(1): 74–89.

[406] Ibid.

[407] Akanle, O. and Shadare, B. R. (2019). Yahoo-plus in Ibadan: Meaning, Characterization and Strategies. *International Journal of Cyber Criminology* 13(2): 343–57.

[408] Adebayo, D. O., Julius, E. and Fasasi, L. (2019). Incidence of Yahoo-Plus activities among in-school adolescents in Delta State, Nigeria. *Global Journal of Guidance and Counseling in Schools: Current Perspectives* 9(1): 14–23.

[409] Ibid.

[410] Premium Times (2022, 2 February). 'Yahoo plus: The new ubiquitous social disorder, By Zainab Suleiman Okino'. Available at: https://www.premiumtimesng.com/opinion/509179-yahoo-plus-the-new-ubiquitous-social-disorder-by-zainab-suleiman-okino.html

[411] This Day Live (2022). Yahoo Plus: Nigerian Youths, Ritual Killings and Quest for Wealth. Available at: https://www.thisdaylive.com/index.php/2022/03/14/yahoo-plus-nigerian-youths-ritual-killings-and-quest-for-wealth?usqp=mq331AQIUAKwASCAAgM%3D

[412] Salu, A. O. (2005). Online crimes and advance fee fraud in Nigeria - are available legal remedies adequate? *Journal of Money Laundering Control* 8(2): 159–67.

Ghana is similar to Nigeria in the use of juju: "Juju priests got Sakawa to drink human blood or potions made with other body parts".[413] This is usually done to ensure that the victim will pay, but fraudsters also access spiritual leaders when they are unable to convince their victims.[414] In these cases, the fraudsters may be given something to put in their mouth while they speak to the victim, or they may be told to do something before calling them.[415] It is understood that Sakawa provides a 'licence' for the fraudster to engage in fraudulent activities.

One interviewee referred to the use of juju as "fraud on steroids".[416] It was also noted that this provides an avenue for the juju priests to also profit from the growth of fraud in both Nigeria and Ghana.[417]

The research identified emerging trends in terms of enhanced technology and the use of spirituality to strengthen frauds. These two trends highlight the current evolution of fraud in Nigeria and Ghana, but there are additional adaptations such as moving to less strict jurisdictions, as has been discussed above.

[413] Mabefam, M. G. and Alexeyeff, K. (2023). Becoming a Sakawa Boy: Magic and Modernity in Ghana. In Y. Musharbash & I. Gershon (Eds.), Living with Monsters: Ethnographic Fiction about Real Monsters (pp. 201–214). Punctum Books. http://www.jstor.org/stable/jj.4391391.1

[414] Interview with an academic, Ghana.

[415] Interview with an academic, Ghana.

[416] Interview with scamfighter.

[417] Interview with scamfighter.

10. Conclusion

Fraud has a long history in Nigeria and India, but it has evolved on different tracks. From early beginnings, when physical letters were used to defraud targets in the UK, Europe, the USA and elsewhere, fraud in Nigeria has evolved to exploit the Internet and its global reach. This cyber-enabled fraud has lowered the barrier to entry to becoming a fraudster and has resulted in multiple different types of fraud being conducted. India, in contrast, has not evolved to take advantage of the Internet; the majority of scams are conducted through call centres. However, this approach provides ready-made infrastructure and staff. The proximity of Ghana to Nigeria provided an opportunity for Nigerian fraudsters to expand, which has resulted in many similarities between the two countries.

In all three countries, fraudsters are agile and innovative and constantly adapt their tactics. New technology is adopted and fraudsters use other mechanisms to enhance their scams, including spirituality, or juju, in the case of Nigeria and Ghana. Innovation and adaptation also occur at a micro level, such as: being able to move to new websites immediately when one is shut down; moving operations to new cities or countries; and reducing the size of scam centres to avoid detection. This requires an equally agile response, and although there is evidence that law enforcement has a good understanding of frauds, prosecutions have not kept pace with scams.

Despite the different techniques for fraud in West Africa and India, the similarities provide entry points to tackle fraud in a systematic way in multiple jurisdictions, although there are nuances that also provide specific responses.

11. References

Aborisade, R. A. (2022). Internet Scamming and the Techniques of Neutralization: Parents' Excuses and Justifications for Children's Involvement in Online Dating Fraud in Nigeria. *International Annals of Criminology* 60(2): 199–219.

Aborisade, R. A. (2022). Yahoo Boys, Yahoo Parents? An Explorative and Qualitative Study of Parents' Disposition towards Children's Involvement in Cybercrimes. *Deviant Behavior* 44(7): 1102–20.

Aborisade, R. A. and Adedayo, S. S. (2021). 'Catch me if you can': the myth and reality of criminals' use of juju to evade arrest from the Nigeria police. *Police Practice and Research* 22(1): 74–89.

Aborisade, R. A., Ocheja, A. and Okuneye, B. A. (2023). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology* 3: 100044.

Abubakari, Y. (2023). The Espouse of Women in the Online Romance Fraud World: Role of Sociocultural Experiences and Digital Technologies. *Deviant Behavior* 45(5): 708–35. DOI: 10.1080/01639625.2023.2263137.

Abubakari, Y. and Blaszczyk, M. (2023). Politicization of Economic Cybercrime: Perceptions Among Ghanaian Facebook Users. *Deviant Behavior* 45(4):483–502.

ActionAid (2023, 27 July). 'Nigerians trafficked to Ghana and forced to work as cyber-criminals for ruthless gangs'. Available at: https://actionaid.org/stories/2023/nigerians-trafficked-ghana-and-forced-work-cyber-criminals-ruthless-gangs

Adebayo, B. (2023, 15 August). 'Sakawa Boys: Meet Ghana's online romance scammers'. Available at: https://www.context.news/digital-rights/sakawa-boys-meet-ghanas-online-romance-scammers

Adebayo, D. O., Julius, E. and Fasasi, L. (2019). Incidence of Yahoo-Plus activities among in-school adolescents in Delta State, Nigeria. *Global Journal of Guidance and Counseling in Schools: Current Perspectives* 9(1): 14–23.

Adejoh, S. O., Alabi, T. A., Adisa, W. B. and Emezie, N. M. (2019). "Yahoo Boys" Phenomenon in Lagos Metropolis: A Qualitative Investigation. *International Journal of Cyber Criminology* 13(1):1–20.

Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian Social Science* 13(4): 19–29.

Adogame, A. (2009). The 419 Code as Business Unusual: Youth and the Unfolding of the Advance Fee Fraud Online Discourse. *Asian Journal of Social Science* 37(4): 551–73.

Ajala, E. B. (2007). Cybercafes, Cybercrime Detection and Prevention. *Library Hi Tech News* 24(7): 26–29.

Akanle, O. and Shadare, B. R. (2019). Yahoo-plus in Ibadan: Meaning, Characterization and Strategies. *International Journal of Cyber Criminology* 13(2): 343–57.

Akeusola, B. N. (2023). Parental Pressure and Cybercrime Engagement among Youth in Nigerian Tertiary Institutions. *KIU Journal of Social Sciences* 9(3): 117–25.

Akinyetun, T. (2021). Poverty, Cybercrime and National Security in Nigeria. *Journal of Contemporary Sociological Issues* 1(2): 86–109.

Akuako, E. (2022). The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana. Available at: https://dr.library.brocku.ca/handle/10464/16385

Ally, A. J. and Gadgala, N. (2022). Addressing Cyber Scam as a Threat to Cyber Security in India. *International Journal of Law Management & Humanities* 5(3): 376–90.

Apantaku, P. O. (2021). Cybercrime: Motivations, Modes, and Emerging Trends, with Nigeria as a Case Study. Doctoral dissertation, University of Portsmouth.

Arewa, A. (2018). Borderless crimes and digital forensic: Nigerian perspectives. *Journal of Financial Crime* 25(2): 619–31.

Arthur-Mensah, G. (2023, 4 September). 'Ghana records GH¢49.5m Ghana Cedis losses through cyber fraud in first half of 2023'. Available at: https://gna.org.gh/2023/09/ghana-records-gh¢49-5m-losses-through-cyber-fraud-in-first-half-of-2023/

Ayub, A. O. and Akor, L. (2022). Trends, Patterns and Consequences of Cybercrime in Nigeria. *Gusau International Journal of Management and Social Sciences* 5(1): 241–62.

Barnor, J. N. B., Boateng, R., Kolog, E. A. and Afful-Dadzie, A. (2020). Rationalizing online romance fraud: In the eyes of the offender. *AMCIS 2020 Proceedings*. 21. Available at: https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/21

Barry, E. (2017). 'India's Call-Center Talents Put to a Criminal Use: Swindling Americans'. Available at: https://www.nytimes.com/2017/01/03/world/asia/india-call-centers-fraud-americans.html?_r=0

BBC World Service (2023). 'Sakawa Boy reveals how scams work – Love, Janessa, Ep3, BBC World Service and CBC Podcasts'. Available at: https://www.youtube.com/watch?v=NOq1SjLVYOQ

Bhattacharjee, Y. (2021, 30 January). 'Who's Making All Those Scam Calls?' Available at: https://go.gale.com/ps/i.do?p=AONE&u=anon~3e957a25&id=GALE|A650038731&v=2.1&it=r&sid=googleScholar&asid=894cc1ea

Button, M., Nicholls, C. M., Kerr, J. and Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology* 47(3): 391–408. doi: 10.1177/0004865814521224.

Campbell, J. (2023, 14 August). '2 Nigerian men accused of running a global 'sextortion' ring linked to a teen's suicide have been extradited to US, officials say'. Available at: https://edition.cnn.com/2023/08/14/us/michigan-sextortion-ring-nigerian-suspects-extradited/index.html

Chaganti, R., Bhushan, B., Nayyar, A. and Mourade, A. (2021). Recent Trends in Social Engineering Scams and Case Study of Gift Card Scam. arXiv preprint. arXiv:2110.06487.

Citi Newsroom (2021, February 18). 'US busts '$50 million Ghana-based cyber fraud scam". Available at: https://citinewsroom.com/2021/02/us-busts-50m-ghana-based-cyber-fraud-scam/

Crowdstrike (2018). Intelligence Report: CSIR – 18004: Nigerian Confraternities Emerge as Business Email Compromise Threat. Available at: https://www.crowdstrike.com/wp-content/uploads/2020/03/NigerianReport.pdf

Dhankar, L. (2023, 2 March). 'Two foreigners held in call centre fraud were planning to flee India, say police'. Available at: https://www.hindustantimes.com/cities/gurugram-news/two-foreigners-held-in-call-centre-fraud-were-planning-to-flee-india-say-police-101677776845652.html

Dokku, S. R. and Kandula, D. (2021). A study on issues and challenges of information technology act 2000 in India. *Annals of Justice and Humanity* 1(1): 39–49. Available at: https://goodwoodpub.com/index.php/ajh/article/view/1389

Economic Times (2021, 4 June). 'How scammers are targeting vulnerable and desperate during India's COVID crisis'. Available at: https://economictimes.indiatimes.com/news/india/how-scammers-are-targeting-the-vulnerable-and-the-desperate-during-indias-covid-crisis/history-of-scams/slideshow/83228982.cms

Edwards, M., Suarez-Tangil, G., Peersman, C., Stringhini, G., Rashid, A. and Whitty, M. (2018, May). The geography of online dating fraud. Paper presented at Workshop on Technology and Consumer Protection, San Franciso, California, United States.

Egole, A. and Okamgba, J. (2023, 5 December). 'Worsening youth unemployment triggers fresh cybercrime, voodoo wave'. Available at: https://punchng.com/worsening-youth-unemployment-triggers-fresh-cybercrime-voodoo-wave/

Ekwenze, S. A. (2012). The Use of the Holy Bible, the Holy Qu'Ran, Juju and Others for Oath of Office: To Fight Corruption in Nigeria. *Law and Religion eJournal*.

Ellis, S. (2016). This Present Darkness: A History of Nigerian Organized Crime. London: Hurst.

Glickman, H. (2005). The Nigerian "419" Advance Fee Scams: Prank or Peril? *Canadian Journal of African Studies* 39(3): 460–89.

Harley, D., Grooten, M., Burn, S. and Johnston, C. (2012). My PC has 32,539 errors: how telephone support scams really work. Virus Bulletin.

Ibrahim, S. (2016). Causes of Socioeconomic Cybercrime in Nigeria. In International Conference on Cybercrime and Computer Forensic (ICCCF): 1–9.

Idem, U. J. (2023). The Legal Approach for Fighting Cybercrimes in Nigeria: Some Lessons from the United States and the United Kingdom. *2023 International Conference On Cyber Management And Engineering (CyMaEn)*.

International Labour Organization (2023). ILO Youth Country Briefs: Ghana. Available at: https://webapps.ilo.org/wcmsp5/groups/public/---ed_emp/documents/publication/wcms_886402.pdf

International Labour Organization (2023). ILO Youth Country Briefs: Nigeria. Available at: https://webapps.ilo.org/wcmsp5/groups/public/---ed_emp/documents/publication/wcms_886409.pdf

International Labour Organization (2024). India Employment Report 2024: Youth employment, education and skills. Available at: https://webapps.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---sro-new_delhi/documents/publication/wcms_921154.pdf

INTERPOL (2023, 8 August). 'Closing ranks on West African organized crime: more than EUR 2 million seized in Operation Jackal'. Available at: https://www.interpol.int/en/News-and-

Events/News/2023/Closing-ranks-on-West-African-organized-crime-more-than-EUR-2-million-seized-in-Operation-Jackal

Irish Independent (2022). 'Explainer: Who are the Black Axe Gang?' Available at: https://www.youtube.com/watch?v=N7TSP3IE2SQ

Ismail, U. (2020). The Nigeria Police Force and Cybercrime Policing: An Appraisal. *Dutse Journal of Criminology and Security Studies* 4(1): 78–88.

Jesperson, S. et al. (2019). Human Trafficking: An Organised Crime? London: Hurst.

Johnson, B. M. (2022, April 10). 'Rise of the scam baiter – fall of the scammers'. Available at: https://www.linkedin.com/pulse/rise-scam-baiter-fall-scammers-bronwyn-may-johnson-mba-/

Khakse, A. and Nambiar, P. (2017). Modern Technology International Crime and Police: An Analysis of Call Centre Crimes in Gujarat. Available at: https://www.academia.edu/38737579/Call_Center_Crimes

Korankye, K. A. (2023, 10 November). 'Scammed – Waiting in pain and in vain; The new way online scammers are tricking unsuspecting customers'. Available at: https://www.graphic.com.gh/news/general-news/ghananewsscammed-waiting-in-pain-and-in-vain.html

Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T. and Okolorie, G. U. (2023). Cheques or dating scams? Online fraud themes in hip-hop songs across popular music apps. *Journal of Economic Criminology* 2: 100033.

Lepkofker, M. (2021). Prosecuting the Phone Scammer When Extradition Fails and Concurrent Jurisdiction Exists. *Brooklyn Journal of International Law* 47(1): 188–231.

Levi, M. (2014). Organized fraud. In Paoli, L. The Oxford Handbook of Organized Crime. Oxford: Oxford.

Liu, J., Pun, P., Vadrevu, P. and Perdisci, R. (2023). Understanding, Measuring, and Detecting Modern Technical Support Scams. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*: 18-38.

Liu, X. M. (2021). A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches. *The Coastal Business Journal* 18(1): Article 2.

Lusthaus, J., van Oss, J. and Amann, P. (2023). The Gozi group: A criminal firm in cyberspace? *European Journal of Criminology* 20(5): 1701–18.

Mabefam, M. G. and Alexeyeff, K. (2023). Becoming a Sakawa Boy: Magic and Modernity in Ghana. In Y. Musharbash & I. Gershon (Eds.), Living with Monsters: Ethnographic Fiction about Real Monsters (pp. 201–214). Punctum Books. http://www.jstor.org/stable/jj.4391391.1

Mathai, A. (2022). 'Ever lost money to digital fraudsters? Join the club'. Available at: https://www.theweek.in/theweek/specials/2022/06/24/ever-lost-money-to-digital-fraudsters-join-the-club.html

Microsoft (2021). Global Tech Support Scam Research. Available at: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2021/07/MSFT-2021-Global-Tech-Support-Scam-Research-Report.pdf

Mohammed, K. H., Mohammed, Y. D. and Solanke, A. A. (2019). Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime* 2(1): 56–63.

Monye, E. (2024, 18 January). 'Why Nigeria's Controversial Naira Redesign Policy Hasn't Met Its Objectives'. Available at: https://carnegieendowment.org/2024/01/18/why-nigeria-s-controversial-naira-redesign-policy-hasn-t-met-its-objectives-pub-91405

The New Indian Express (2019, October 21). 'UK, India police shut down Kolkata call centres in major online fraud probe'. Available at: https://www.newindianexpress.com/world/2019/Oct/21/uk-india-police-shut-down-kolkata-call-centres-in-major-online-fraud-probe-2050888.html

Office of Public Affairs (2016, 27 October). 'Dozens of Individuals Indicted in Multimillion-Dollar Indian Call Center Scam Targeting U.S. Victims'. Available at:

https://www.justice.gov/opa/pr/dozens-individuals-indicted-multimillion-dollar-indian-call-center-scam-targeting-us-victims#:~:text=Today%2C%20an%20indictment%20was%20unsealed%20charging%20a%20total,in%20hundreds%20of%20millions%20of%20dollars%20in%20losses.

Oduro-Frimpong, J. (2014). Sakawa rituals and cyberfraud in Ghanaian popular video movies. *African Studies Review* 57(2): 131–47.

Ogune, M. (2023, 28 June). 'EFCC Secures Conviction of Two Internet Fraudsters in Abuja'. Available at: https://guardian.ng/news/efcc-secures-conviction-of-two-internet-fraudsters-in-abuja/

Ogune, M. (2023, 28 June). 'Notorious internet fraudster to spend 235 years imprison for N252million fraud'. Available at: https://guardian.ng/news/notorious-internet-fraudster-to-spend-235-years-imprison-for-n525million-fraud/

Ogune, M. (2023, 18 July). 'Court sends four internet fraudsters to prison in Benin City'. Available at: https://guardian.ng/news/court-sends-four-internet-fraudsters-to-prison-in-benin-city/

Ogunleye, Y. O., Ojedokun, U. A. and Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology* 13(2): 309–25.

Ohuocha, C. (2024, 26 February). 'Nigeria outlaws street-trading by FX bureaus in new rules to stem naira slide'. Available at: slidehttps://www.cnbcafrica.com/2024/nigeria-outlaws-street-trading-by-fx-bureaus-in-new-rules-to-stem-naira-slide/

Okpe, V. V. and Taya, S. L. (2018). Political Perspective: Evaluating the Causes of Cybercrime in Nigeria. *Asian Journal of Multidisciplinary Studies* 6(12): 42–52.

Peace, F. W., Egharevba, M. E. and George, T. O. (2022). Sociological Investigation of Factors Driving Cybercrime Among Undergraduates with Severe Implication in the Educational System in Nigeria. *Proceedings of SOCIOINT 2022 – 9th International Conference on Education & Education of Social Sciences*.

Poonam, S. (2018, 2 January). 'The scammers gaming India's overcrowded job market'. Available at: https://www.theguardian.com/news/2018/jan/02/the-scammers-gaming-indias-overcrowded-job-market

Premium Times (2022, 2 February). 'Yahoo plus: The new ubiquitous social disorder, By Zainab Suleiman Okino'. Available at: https://www.premiumtimesng.com/opinion/509179-yahoo-plus-the-new-ubiquitous-social-disorder-by-zainab-suleiman-okino.html

Ribic, P. (2019). The Nigerian email scam novel. *Journal of Postcolonial Writing* 55(3): 424–36.

Rich, T. (2018). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal* 31: 208–25.

Richards, N. U. and Eboibi, F. E. (2023). Cybercrime perspectives to the 'ENDSARS' protest in Nigeria. *African Security Review* 32(1): 38–56.

RNZ (2018, 14 January). 'The desperation of India's scammers'. Available at: https://www.rnz.co.nz/national/programmes/up-this-way/audio/2018628439/the-desperation-of-india-s-scammers

Rubinsztein-Dunlop, S., Robinson, L. and Dredge, S. (2019). 'Meet the scammers: Could this be your online lover?' Available at: https://www.abc.net.au/news/2019-02-11/ghana-meet-the-scammers/10785676

Salu, A. O. (2005). Online crimes and advance fee fraud in Nigeria - are available legal remedies adequate? *Journal of Money Laundering Control* 8(2): 159–67.

Sherry, A. (2023, 14 August). 'Faces of Black Axe international fraud gang members after being busted in Ireland'. Available at: https://www.sundayworld.com/crime/irish-crime/faces-of-black-axe-international-fraud-gang-members-after-being-busted-in-ireland/a357806436.html

Srinivasan, B., Kountouras, A., Miramirkhani, N., Alam, M., Nikiforakis, N., Antonakakis, M. and Ahamad, M. (2017). By Hook or by Crook: Exposing the Diverse Abuse Tactics of Technical Support Scammers. arXiv preprint arXiv:1709.08331.

Srinivasan, B., Kountouras, A., Miramirkhani, N., Alam, M., Nikiforakis, N., Antonakakis, M. and Ahamad, M. (2018, April). Exposing search and advertisement abuse tactics and infrastructure of technical support scammers. *WWW '18: Proceedings of the 2018 World Wide Web Conference*: 319–28.

This Day Live (2022). Yahoo Plus: Nigerian Youths, Ritual Killings and Quest for Wealth. Available at: https://www.thisdaylive.com/index.php/2022/03/14/yahoo-plus-nigerian-youths-ritual-killings-and-quest-for-wealth?usqp=mq331AQIUAKwASCAAgM%3D

Times of India (2023, 20 October). 'CBI launches Operation Chakra-II: What it is and why Microsoft and Amazon are part of this'. Available at: https://timesofindia.indiatimes.com/gadgets-news/cbi-launches-operation-chakra-ii-what-it-is-and-why-microsoft-and-amazon-are-part-of-this/articleshow/104582380.cms

Tookitaki (2023, 4 December). 'Cyber Fraud: Real-Life Examples and Prevention Strategies'. Available at: https://www.tookitaki.com/compliance-hub/cyber-fraud-real-life-examples-and-prevention-strategies

Tzani Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R. and Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. *Journal of Forensic and Investigative Accounting* 12(1): 163–78.

UK government (2023). Fraud Strategy: Stopping Scams and Protecting the Public. Available at: https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf

UK government (2024). 'Policy paper: Global Fraud Summit Communiqué: 11 March 2024'. Available at: https://www.gov.uk/government/publications/communique-from-the-global-fraud-summit/global-fraud-summit-communique-11-march-2024

United States Attorney's Office (2020, 26 August). 'Ghanaian Citizen Extradited in Connection with Prosecution of Africa-Based Cybercrime and Business Email Compromise Conspiracy'. Available at: https://www.justice.gov/usao-wdtn/pr/ghanaian-citizen-extradited-connection-prosecution-africa-based-cybercrime-and-business

UNODC (2022). Organized Crime in Nigeria: A Threat Assessment. Available at: https://www.unodc.org/conig/uploads/documents/NOCTA_Web_Version_25.09.2023.pdf

UNODC (2023). 'India: UNODC Joins Forces with India's Ministry of Home Affairs for the G20 Conference on Cyber Security'. Available at: https://www.unodc.org/southasia//frontpage/2023/July/india_-unodc-joins-forces-with-indias-ministry-of-home-affairs-for-the-g20-conference-on-cyber-security.html

Vaidyanathan, R. (2020, 8 March). 'Confessions of a call-centre scammer'. Available at: https://www.bbc.com/news/stories-51753362

Van Nguyen, T. (2022). The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. *Trends in Organized Crime* 25(2): 226–47.

Wen, N. J., Carolyn, M., Ang, J., Jingmin, H. and Shuyan, O. (2021). Uncovering the Workings of Credit-for-Sex Scams. Available at: https://www.mha.gov.sg/docs/hta_libraries/publications/07-crime.pdf

WION (2023, 19 June). 'Delhi Police, FBI bust call centre scam which conned US citizens of $20 million'. Available at: https://www.wionews.com/world/delhi-police-fbi-bust-call-centre-scam-which-conned-us-citizens-of-20-million-605848

We provide expert monitoring, evaluation, learning and strategy services to help build a more equitable and sustainable world for all.

itad.com | @ItadLtd | Itad | mail@itad.com

Itad Ltd
International House
Queens Road
Brighton, BN1 3XE
United Kingdom

Tel: +44 (0)1273 765250

Itad Inc
c/o Open Gov Hub
1100 13th St NW, Suite 800
Washington, DC, 20005
United States