INTER-GOVERNMENTAL ACTION GROUP AGAINST MONEY LAUNDERING IN WEST AFRICA

REGIONAL REPORT

TYPOLOGIES OF MONEY LAUNDERING AND TERRORIST FINANCING LINKED TO CYBERCRIME IN WEST AFRICA

May 2025

The Inter-Governmental Action Group against Money Laundering (GIABA) is a specialized institution of ECOWAS and a FATF Style Regional Body that promotes policies to protect member States financial system against money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter terrorist financing (CTF) standard.

For more information about GIABA, please visit the website: www.giaba.org

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city, or area.

Citing reference:

GIABA Typologies Report (2025), Money Laundering and Terrorist Financing Linked to Cybercrime in West Africa, GIABA, Dakar, Senegal

ACKNOWLEDGEMENT

The Director General would like to acknowledge the support provided by the GIABA member States in the conduct of this typologies study. GIABA is particularly grateful to its National Correspondents (NCs) and the country researchers for their efforts in the data collection process, especially by mobilizing national stakeholders and facilitating a timely access of the research team with the relevant agencies and institutions at national levels.

The study benefited from the enormous support of the law enforcement agencies, intelligence services, the judiciary, other professional bodies and civil societies of member States. These institutions/agencies ensured that the research team met with key stakeholders and provided required information, in some cases at very short notice.

GIABA would also like to recognize the exceptional collaboration by our development partners, particularly the FATF and OCWAR-C, for taking their time to review the report at various stages and thereby enriching it. The members of the GIABA Risk, Trends and Methods Group (RTMG) and Policy Review Group (PRG) also worked collaboratively with the Secretariat to improve the overall quality of this report.

We also wish to acknowledge the efforts of the individual project team members, who worked round the clock to ensure proper coordination and delivery of the Project, under the supervision of the Director of Policy & Research, Mr. Muazu Umaru. Our special thanks also goes to our colleague Mr. Lansana Daboh (Risk Monitoring Officer) whose commitment has been instrumental in the production and finalization of this report. Other members of the research team worth acknowledging are Madam Mairo Ladidi Abass, Madam Ramatoulaye Barry Diop, Mr. Saer Kamara and Mr Idrissa Ouattara.

GIABA Secretariat

TABLE OF CONTENTS

LIST OF ABBREVIATIONS AND ACRONYMS

AI:	Artificial Intelligence
ML:	Money Laundering
AML:	Anti-money Laundering
TF:	Terrorism Financing
CFT:	Counter Terrorism Financing
PF:	Proliferation Financing
CFP:	Counter Proliferation Financing
IoT:	Internet of Things
FIU:	Financial Intelligent Unit
NRA:	National Risk Assessments
AUC:	African Union Commission
EFCC:	Nigeria's Economic and Financial Crimes Commission
GIABA:	Intergovernmental Action Group against Money Laundering in West Africa
ECOWAS:	Economic Community of West African States
ECG:	Evaluation and Compliance Group
RTMG:	Risks Trends and Method Group
PRG:	Policy Review Group
MER:	Mutual Evaluation Report
DDOS:	Distributed Denial of Service
BEC:	Business Email compromise
NPF:	Nigeria Police Force
EOCO:	Economic and Organized Crime Office
STR:	Suspicious Transaction Report
VA:	Virtual Asset
VASP:	Virtual Asset Service Provider
ICT:	Information and Communication Technology
LTA:	Liberia Telecommunication Agency
FIA:	Financial Intelligent Center
NFIU:	Nigeria Financial Intelligent Unit
OCWAR-C:	Organized Crime: West Africa Response on Cybersecurity and Cybercrime
FATF:	Financial Action Task Force
NATCOM:	National Telecommunication Commission
BoG:	Bank of Ghana
EU:	European Union

EXECUTIVE SUMMARY

1. The digital attack surface has vastly expanded from a move to remote work, from more people coming online, and from more interconnectivity of computers and smart devices around the globe. With the development of digital technologies, the use of information and communications networks as a tool for facilitating illicit financial flows is rising as one of the key challenges in tackling the problem of the movement of illegal funds. New digital tools for money transfers, such as online and mobile banking, electronic payments, cryptocurrencies, e-commerce providers, and online gambling services, especially if they are combined, provide a countless number of opportunities to distance money from illegal sources of profit or to illegally transfer money from legal sources. The COVID-19 pandemic also created new opportunities for criminals to abuse the financial systems through technologies in a more innovative and complex manner.

2. In view of the foregoing, it is very clear that digital technologies pose significant problems to combatting money laundering, organized crimes and terrorist financing as cyber-attacks continue to evolve and increase in frequency and sophistication. All GIABA's recent reports glaringly reveal the prevalence of cybercrimes, both as a major source of proceeds of crime and as a vehicle of criminal funds in the region. It appears that all types of crimes associated with digital technologies in the region are systematically difficult to deal with not only because of the regulatory and law enforcement gaps but also due to the lack of adequate expertise and infrastructures. In most GIABA member countries, cybercrime is a serious threat to national economies that requires a coherent and collaborative response at a regional level. Standards also need to be agreed upon and harmonised internationally to reduce the risk of gaps and regulatory arbitrage.

3. Cognizant of this complex challenge, GIABA conducted this typologies study on Money Laundering and Terrorist Financing linked to Cybercrime in West Africa. Despite the seriousness of this phenomenon, Cybersecurity is still considered to be a luxury, not a necessity in many African economies. Its importance has not yet been sufficiently appreciated or acknowledged. In view of the preceding, the conduct of such typologies exercise is imperative. This will fuel the basis of a structural and regulatory foundation of combatting computer-based crimes in West Africa.

4. The study aims to enhance understanding on the money laundering risks linked to cybercrime among GIABA member States; to provide enhanced policy, compliance and enforcement. The findings will reveal the implications for interventions and relevant recommendations will be proffered in that respect. The report sets to throw light on the differences between cybersecurity and cybercrimes and the magnitude of both phenomena in West Africa and the prevalence of the crime. It will explore the ML/TF risks factors associated with cybercrimes in the region and map out the most common techniques and methods adopted to launder the proceeds of cybercrime. It will point out the most critical vulnerabilities leading to heightened risks of laundering the proceeds of cybercrime and proffer policy measures and action-oriented programmes that can be adopted based on the findings of the study.

5. The methodology adopted was a multi-stakeholder approach including the GIABA Secretariat, expert groups and one expert from the member States. The main findings of the study include a dichotomy between cybersecurity and cybercrime, the prevalent nature of cyber cases and the methods, techniques and trends of the crime in West Africa. The study revealed that West Africa has witnessed a surge in internet connectivity above the Sub-Sahara Africa average. This connectivity is however, variable and dispersed. The connectivity rate in West Africa is as high as 70% (Cabo Verde) and low as 15% (Niger). The gains made in relation to the surge in internet connectivity is being eroded by the exponential rate at which cybercrime is being perpetrated and consequences are dire and damaging.

6. Based on interviews conducted by country researchers, there is a convergence view that law enforcements throughout the region seems overwhelmed as 2 out of every 3 offences reported is related to cybercrime. This was more evident during the peak of the COVID 19 period (2020 – 2021). A diagram in Chapter 2 gives a pictural evidence

of the prevalence of cybercrime in West Africa and depict the extent (estimate) at which the various case types are being perpetrated. The most prevalent of the cases (40%) falls under the advance fee fraud type. Next is mobile money related (15%) cases type, followed by Ponzi scheme (13%) cases type. The next most prevalent case types are website or business platform hacking (7%), and DDOS and businesses email compromise (7%) cases combined. The least cases reported are credit/debit card fraud and TF related cases.

7. There were seven distinct typologies abstracted from the 52 identified cases that appear to describe the phenomenon. The typologies include electronic cards (credit/debit) fraud; email compromise scam/fraud; hacking and defrauding business/organisation's systems; advance fee fraud; Ponzi scheme fraud; mobile money related fraud; and cyber enabled terrorist financing cases. The indicators and red flags confirm that informalities, lack of awareness of cyber threats by the public, inadequate resources invested into cyber security by businesses and public institutions/organizations, weak architecture, and regulatory systems and monitoring of the cyber landscape in the region, and weak enforcement systems has a spiral effect on cyber and cyber enabled crime, money laundering and terrorist financing in West Africa.

8. There are significant legislative gaps in countries, particularly around the powers of the central authority in charge of the fight against cybercrime and around the legal and enforcement frameworks of countries to effectively detect, prove and curb ML or TF associated with cybercrime. While the legal and enforcement framework make provisions for law enforcement action to investigate and prosecute cyber criminals, the regulatory framework in most of West Africa either have insufficient preventive measures or is weak overall. Although few countries have made some gains on obtaining electronic and digital evidence during investigation. This continue to be a challenge in some jurisdictions.

9. In line with global standard requirements particularly, under the FATF Recommendation 36 on International Cooperation which encouraged countries to ratify other relevant international instruments and conventions, such as the Budapest Convention and Malabo Conventions. the West Africa region has made considerable effort and progress in the fight against cybercrime, alongside other predicate offences. But this effort and progress has not been free from challenges. It includes issues such as gaps in laws, institutions misunderstanding their mandate, limited technical capacity, inadequate human and material resources and a lack of collaboration and coordination. Also, international cooperation is still very weak.

10. Although there is a wide range of methods and techniques used by cybercriminals to launder the proceeds of their criminal activities, investigators and prosecutors have conducted few or no parallel financial investigations when cybercrime is detected. They are also confronted, in many cases, with the difficulty of establishing proof of the cybercrime offence due to a lack of the required technology and equipment, ineffective integrated national coordination between AML/CFT operational units and a lack of implementation of regional and international cooperation mechanisms.

11. For the fight against cybercrime to be more effective and deterrent, the study put forward recommendations for both the public and competent authorities fighting against cybercrime. There is need to initiate and intensify awareness-raising campaigns for the public; promote a culture of cybersecurity in the region and support countries in the establishment of a legal and institutional framework in accordance with international standards currently in force. Conduct proper risks assessment and set up Digital Forensic Laboratories to support forensic evidence for LEAs. Strengthen the operational capacities of investigators on digital investigation techniques and bridge the gap between the legal framework and the Special AML/CFT/CFP laws to facilitate and fast track the criminal prosecution of cybercrime offences.

12. Set up a Regional Forum of National Platforms to Combat Cybercrime in West Africa to allow competent authorities to network, share information and intelligence. Monitor the signing, ratification and domestication of international instruments and build capacity in detection, investigation, prosecution, and adjudication of cybercrime cases and how to follow the money, including undertaking parallel and financial investigations.

CHAPTER 1

INTRODUCTION

Background

13. Emerging technologies such as Self-driving cars, Artificial Intelligence (AI), Machine Learning, Automation, Virtualization, Smart Cities, Blockchain Networks, Big Data, Internet of Things (IoT), Internet of Senses, Cloud and Quantum Computing, etc. are creating operational shifts that will require new cybersecurity requirements. In the past couple of years, the digital attack surface has vastly expanded due to a move to remote work, more people coming online, and more interconnectivity of computers and smart devices around the globe.

14. Simultaneously, criminal enterprises have taken advantage of the lack of visibility and security administration. With the development of digital technologies, the use of information and communications networks is rising as a tool for facilitating illicit financial flows. This is one of the key challenges in tackling the problem of the movement of illegal funds. It goes without saying that digital technologies facilitate illicit financial flows at each stage, be it earning money illegally, transferring illegal funds, or using them. There are several areas where clear links between technology and illicit financial flows can be established.

15. In addition to the creation of the underground illegal markets of cybercrime and cyber-related crime, digital technologies facilitate the migration of traditional organized crime online and provide several opportunities for fraud, corruption, tax evasion, amongst other criminal activities. New digital tools for money transfers, such as online and mobile banking, electronic payments, cryptocurrencies, e-commerce, and online gambling provide a countless number of opportunities to distance money from illegal sources of profit or to illegally transfer money from legal sources, especially if they are combined.

16. Also, new forms of doing business online and the digital economy facilitate the transfer of illegal profits and the aggregation of illicit funds in offshore accounts, their placement in fake e-commerce companies and offshore online businesses. The COVID-19 pandemic also created new opportunities for criminals to abuse the financial systems through technologies in a more innovative and complex manner.

17. In view of the foregoing, it is very clear that digital technologies pose significant problems to combatting money laundering, organized crimes and terrorist financing. Cyber-attacks continue to evolve and increase in frequency and sophistication. That is the reason why cybercrime has become a major area of attention and investment across the world.

18. In West Africa, the nexus between money laundering/terrorist financing (ML/TF) and cybercrimes is blatant. While ML/TF developed due to financial globalisation (i.e., the ability for all economic and social actors to use financial services internationally), cybercrime is growing due to technological globalisation through the development of the Internet and related tools. GIABA's report on Fintech deployment, frequent news headlines, annual activity reports submitted by GIABA member States and their reports on National Risk Assessments (NRA) of ML/TF, outcomes of mutual evaluations, and follow-up processes, all glaringly reveal the prevalence of cybercrimes, both as a major source of proceeds of crime and as a vehicle of criminal funds in the region. It appears that all types of crimes associated with digital technologies in the region are systematically difficult to deal with not only because of the regulatory and law enforcement gaps but also due to the lack of adequate expertise and infrastructures.

19. In most GIABA member countries, cybercrime is a serious threat to national economies that requires a coherent and collaborative response at a regional level. Some jurisdictions' failures to fight cybercrime threaten the security, stability and effectiveness of governments, critical infrastructures, businesses, and individuals around the region. It requires resilient governance to ensure that relevant agencies in all jurisdictions cooperate (e.g., between supervisors, FIUs and other operational bodies on crime prevention or law enforcement). National Standards also need to be agreed upon and possibly harmonised regionally, if not internationally to reduce the risk of gaps and regulatory arbitrage, mostly for cross border purposes. Besides, the lack of consistency and harmonisation between jurisdictions has driven compliance costs.

20. Cognizant of this complex challenge, GIABA conducted this typologies study on Money Laundering and Terrorist Financing linked to Cybercrime in West Africa.

Motivation for the Study

21. Most African economies are characterised by regulatory regimes' permissiveness that provides a fertile ground for cybercrime activities. According to a November 2016 report of the African Union Commission (AUC) and the cybersecurity firm Symantec, out of the 54 countries of Africa, 30 lacked specific legal provisions to fight cybercrime and dealing with electronic evidence. Law enforcement officials in some countries do not take significant actions against hackers attacking international websites. For instance, it was reported that some officials in Nigeria claimed that they were unaware of cybercrimes originating from the country, while some labelled it as western propaganda. Some elected high-level State officials were also reportedly involved in cybercrimes. In 2003, Nigeria's Economic and Financial Crimes Commission (EFCC) arrested a member of Nigeria's House of Representatives for his alleged engagement in cybercrime-related activities.

22. The classification of cybercrime cases according to the countries of origin (AUC, 2016) of complainants mentions three African countries among the 50 most affected: they are South Africa in the 11th place (434 complaints), Nigeria (24th place, with 215 complaints) and Egypt (45th, 95 complaints). When the cases are classified according to the damages caused, South-African complainants are again in the first position with 6.5 million dollars lost, followed by Nigeria (2,9 million dollars) and Egypt (523.000 dollars). The emergence of these crimes linked to transactions by phone is made more accessible by the widespread use of mobile money payments methods.

23. Regarding sim box fraud, it cost 926 million CFA francs for Côte d'Ivoire in 2014. This technique allows the fraudsters to bypass international telecommunications' usual channels, which are then treated as local calls, resulting in rate arbitrage. This causes enormous losses for telecom companies. In Senegal, although little data is available, the most significant case involves a money transfer company whose website was hacked for several hours in 2020. The hackers, who said they were Senegalese, wanted to draw attention to the matter of security. The frontpage of the site had a black page with a text by the two perpetrators. They said, among other things, that cyber security is neglected in the country and their action was undertaken to remind those concerned of the importance of cyber security.

24. Despite the seriousness of this phenomenon, Cybersecurity is still considered to be a luxury, not a necessity in many African economies. Its importance has not yet been sufficiently appreciated or acknowledged. Cybersecurity budgets in many organisations are reported to be less than 1%, and many organisations had a zero-budget allocated to cybersecurity. Yet, digital technologies have the potential to serve as a tool to tackle the problem of money laundering and terrorism financing. They can serve as a source of empowerment and transparency, and could be used in investigations, detection, and disruption of the illegal money transfers.

25. In view of the preceding, the conduct of a thorough typologies exercise is imperative. This will fuel the basis of a structural and robust regulatory foundation for combatting computer-based crimes in West Africa. It will further throw light on the threats of cybercrime and the extent to which it is exacerbating other money laundering predicate crimes, including that of money laundering and terrorist financing in the GIABA region.

Objective

26. The typologies study aims to enhance understanding of the money laundering risks linked to cybercrime among GIABA member States; it aims to provide enhanced policy, compliance and enforcement. The findings will reveal the implications for interventions and relevant recommendations will be proffered. The report sets to address the following specific issues:

a) What are the differences between cybersecurity and cybercrime? And what is the magnitude of related phenomena in West Africa?
b) What are the different forms of criminal activities through digital technologies in GIABA member States?
c) What are the ML/TF risks factors associated with cybercrimes in the region?
d) What are the most common techniques and methods adopted to launder the proceeds of cybercrime activities in West Africa?
e) What are the most critical (systemic) vulnerabilities leading to heightened risks of laundering the proceeds of cybercrime?
f) What are the policy measures and action-oriented programmes that can be adopted based on the findings of the study to effectively mitigate the risks of ML/TF associated with digital technologies?

Study Methodology

27. As a prelude to the methodology, the study was conceived during the several engagements and discussions at GIABA technical forums and meetings of its various reports (RTMG/PRG and ECG experts' and Plenary meetings) - discussions during the MERs, Fintech assessment report, Risks Assessment particularly VA & VASP) between 2021 and early 2022. The detailed methodology adopted afterwards include the following:

A **3-day brainstorming session** was organized in **July 2021** to reflect on the main problems related to this issue as well as the scope of the project. The session considered presentations of representatives from member States on the prevailing situation of cybercrime in their respective countries. The RTMG/PRG members also contributed to that effect.

A virtual brainstorming session was held in **September 2021** and the outcome of those two (2) sessions helped in finalising the project concept and the detailed Terms of Reference to recruit the project team members from the GIABA member States.

A project team was constituted, consisting of 15 Country Researchers (one expert recruited from each ECOWAS member State), the GIABA RTMG and PRG members, and supported by the GIABA Secretariat in **July 2022**.

Data collection and analysis (administering of questionnaires, including conducting in-depth interview with a range of relevant authorities, anti-cybercrime agencies, financial institutions as well as victims of cybercrimes and other vulnerable individuals) – (**July-September 2022**).

Review of country reports submitted by experts and extensive analysis of the patterns, methods, techniques and impact of the phenomenon and a critical analysis of findings, including follow–up at country level as may be required–**September-October 2022**.

Consideration of the country reports at the GIABA Annual Regional Typologies Exercise Workshop – **October 2022**.

Drafting of a comprehensive report, including specific and general recommendations that would assist in policy formulation and operational interventions against ML/TF linked to cybercrimes at both the national and regional levels – **March-April 2023**.

Translation and quality review of the draft consolidated report into the 3 ECOWAS languages – **April - May 2023**.

Offsite review and validation by member States, observers, development partners RTMG/PRG members, and other stakeholders – **May 2023**.

Consideration and approval of the report by the GIABA plenary - **May 2023**.

CHAPTER 2

THE PREVALENCE OF CYBERCRIME IN WEST AFRICA

28. This chapter attempts to review and present the extent and types of cybercrime perpetrated in the West African region, considering the volume of cybercrime cases being reported on daily basis and the (in)ability of law enforcement to investigate every case. It is also worth noting that the number of cases or incidences reported to law enforcements does not necessarily translate into investigations, as several reported cases or incidences (tens and hundreds of reports) could be related and result in a single case. The chapter will look at some contextual and definition issues before discussing the types of cases prevalent in the region, as reported.

Dichotomy Between Cybercrime and Cyber Security

29. Cybercrime is a criminal activity that involves a computer, network device or network, directly targeted to damage or disable computers and devices, spreading malware for example, stealing secret information, etc., mostly committed for profit generating purposes. Cybercrimes occurs wherein a computer / network device / network is (a) targeted, or (b) being incidental to the crime, or (c) being used directly to perpetrate the crime. While (a) and (b) are mostly due to vulnerabilities in the system, (c) is a direct threat to the system. Also, while (a) has to do with the level of cybersecurity alertness, awareness, and preparedness of the public (all natural and legal persons), (b) involves the policy, regulatory and law enforcement ability to prevent and disrupt cybercrime, including the effective management of the jurisdictional cyber architecture and environment (public domain).

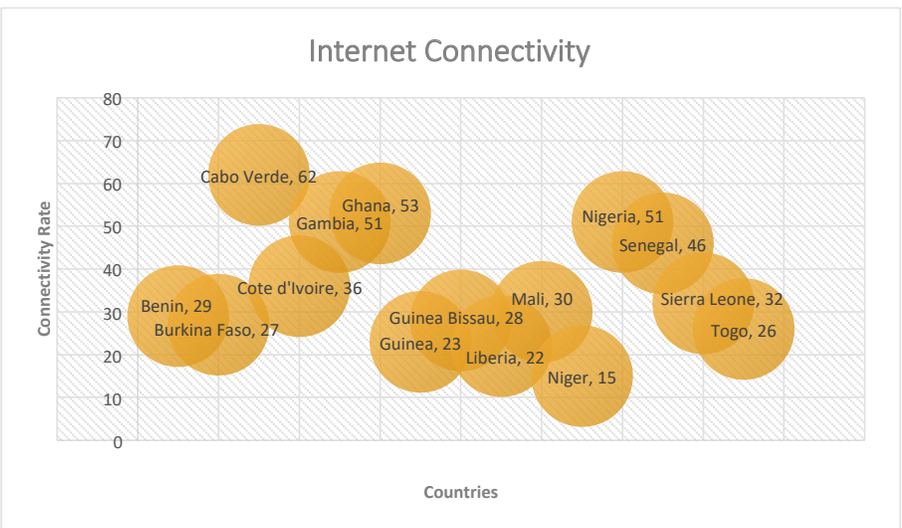
30. Cyber Security is the technology and process that is designed to protect networks and devices from attacks, damages, or unauthorised access. Cyber security aims at protecting organizations thereby increasing efficiency and productivity, inspiring client/partner confidence. Aspects of Cyber security include , data protection and securing an organisations systems to prevent attacks. Cyber security is an important operational requirement for any economic actor and is mostly required for three (3) key reasons, i.e., the principles of confidentiality (information and functions to be accessed only by authorized parties), integrity (information and functions to be added, altered, or removed only by authorized parties) and availability of information (systems, functions, and data must be available on demand according to agreed-upon parameters based on levels of service).

31. Preventing and disrupting cybercrime is an important effect of cyber security. The process of ensuring a system is secured against intrusion and abuse is not just limited to taking the various steps of having multilayers of authentications and complex password, firewalls, and antiviruses with encryption on secured domain names servers, but also, conducting regular updates and assessing risks (identify, monitor, and evaluate threats), and putting in place mitigants for identified risks. Although cybersecurity may help prevent certain cybercrimes not all cyber (enabled) crimes can be prevented with good security alone.

Prevalence of Cybercrime in West Africa

32. Although the study (in the next chapter) presents the various types of typologies present in West Africa, this section presents the prevalence of the crime without diving into the detailed techniques and methods used to perpetrate the crime. West Africa has witnessed a surge in internet connectivity above the Sub-Sahara Africa average. This connectivity is however, variable and dispersed. The connectivity rate in West Africa is as high as 70% (Cabo Verde) and low as 15% (Niger). The gains made in relation to internet connectivity lead to an exponential rate at which cybercrime is being perpetrated. Its consequences are dire and damaging. Below is a diagram (Figure2.1) showing internet connectivity rate in the region.

Figure 2.1: Internet Connectivity in West Africa



33. Based on interviews conducted by country researchers, there is a convergence view that law enforcements throughout the region seems overwhelmed as 2 out of every 3 offences reported is related to cybercrime. This was more evident during the peak of the COVID 19 period (2020 – 2021). The diagram below gives a pictural evidence of the prevalence of cybercrime in West Africa and depict the extent (estimate) at which the various case types are being perpetrated. The most prevalent of the cases (40%) falls under the advance fee fraud type. Next is mobile money related (15%) cases type, followed by Ponzi scheme (13%) cases type. The next most prevalent case type website or business platform hacking (7%), and DDOS and businesses email compromise (7%) cases combined. The least cases reported are credit/debit card fraud and TF related cases.

Figure 2.2: Prevalence and Crime Type in West Africa

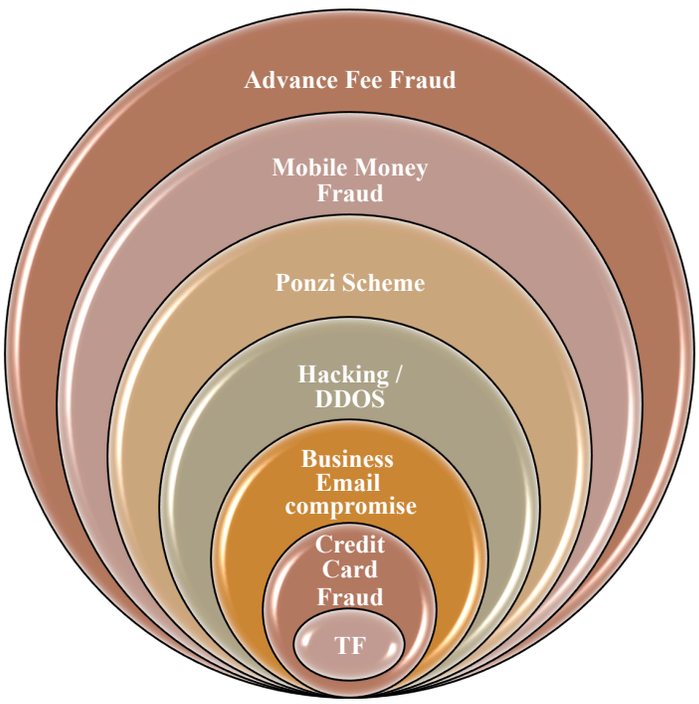


Table 2.1: Prevalence and Crime Type with Weighted Average in West Africa

Crime Type	Weighted Average	Specific description / title of crime
Advance Fee Fraud	0.39	Gold scam, sextortion, child pornography, extorsion, front/shell company romance scam, job recruitment scam, business proposal scam, export contract scam, freight service scam, inheritance scam, human trafficking and kidnapping, forgery and blackmail, fraud and impersonation
Mobile Money Fraud	0.15	False pretence, impersonation and forgery, sim card fraud, insider dealing and hacking, mobile money agent fraud, identity theft through pre-activated sim from abandon voters' record
Ponzi Scheme Fraud	0.14	Online trading scheme, Ponzi scheme fraud, Virtual asset Ponzi scheme, online investment / securities market scam, mobile money investment Ponzi scheme, e-commerce investment scam, online loan scam
Hacking/ DDOS	0.12	Hacking website, hacking business platform, DDOS, Insider dealing / Compromised employee, hacking social media account and impersonation, insider dealing and fraudulent credit facility scheme
Business Email compromise	0.10	BEC, phishing and email scam
Credit Card Fraud	0.06	Credit / debit card theft, credit / debit card fraud
TF Related	0.06	Trade based TF, suspected fund raising for TF, hawala for TF

CHAPTER 3

TYPOLOGIES CASE STUDIES ON ML AND TF CYBERCRIME IN WEST AFRICA

34. This chapter deals with the various typologies observed from the cases submitted. There are 52 cases from seven different typologies as presented below. The typologies include electronic cards (credit/debit) fraud; email compromise scam/fraud; hacking and defrauding business / organisation's systems; advance fee fraud; Ponzi scheme fraud; mobile money related fraud; and cyber enabled terrorist financing cases.

Typology 1: Electronic Cards (credit/debit) Fraud

35. There are 3 cases identified under this typology from the cases submitted. The cases involved wire fraud, stealing credit / debit card details and luring victims to pay for products that are non-existent through fake online marketing.

Case 1: Credit / Debit Card Fraud and the use of Shell Company

A source filed a complaint with the FIUL alleging wire fraud and money laundering by Korlane Investment Limited Liability Company and its corporate owners. A full-scale investigation into the allegation was conducted by LEA. The Investigators found that Korlane Investment Limited Liability Company operated a shell company in Liberia without office, staff, etc., opened and used its accounts in Liberia to launder, conceal and direct stolen funds generated through unusual transactions from wire fraud – a predicate crime of money laundering. The suspects were indicted for money laundering, property theft, wire fraud, and criminal conspiracy.

Upon obtaining a writ of arrest by the prosecutor, the perpetrators evaded being arrested and absconded the country. A motion to confiscate the proceeds was filed consistent with the Provisional Remedies Proceeds of Crimes Act 2013. The motion was assigned for hearing and argued. The Court granted the motion and ordered the proceeds of over US$234,000 confiscated and transferred to GOL. The technique used by the cybercriminal was the use of E-Money platform Credit Card (swift, Visa, and MasterCard) to fraudulently carry out transactions. The criminal manipulated the master card to exceed bank threshold. Such scheme used is known as an International Credit card fraud which is noncompliant with MasterCard Standards.

Source: Liberia

Case 2: Credit / Debit Card Fraud and Fake Import / Export Transaction

The accused, the owner of a company which was into agricultural products and farm implements operated four accounts with a particular bank. Between January 24, 2017, and March 31, 2017. The accused, who was involved in credit card fraud created an online marketing website, through which he received several orders, mostly from the USA, for the supply of Agricultural products. The accused enrolled on the banks online payment platform which enables unsuspecting customers to make payments directly to his account for goods ordered. Within two months, the accused received GHS1,468,447.59 (USD341,500) into his account from several credit cards from different jurisdictions. However, his bank received Visa and MasterCard chargebacks from the Bank of America that some of the payments made to the company were not authorised by the card owners and hence fraudulent. During due diligence carried out by the bank, the accused claimed that funds were proceeds from export of agricultural products that he had shipped through shipping agencies to customers.

Investigations however revealed that the shipping agencies mentioned had not shipped those products and that the cargo airway bills submitted to support his claims were all fake. As a result, a suspicious transaction report (STR) was filed with the FIC. The accused, dissatisfied with the bank's decision to hold onto the funds, reported the bank to EOCO for holding his funds without justification. Unknown to the accused, EOCO had already received intelligence from FIC to investigate the accused. EOCO collaborated with the FBI and SFO to engage with the victims and a prima facie case established against the accused which indicated that the credit cards from which the payments were received by the accused were stolen cards.

Consequently, the accused was slapped with charges including tax evasion, money laundering and defrauding by false pretences. During prosecutions, five of the victims testified through video conferencing via Skype to confirm that indeed they had not purchased goods from the accused and that their credit cards were fraudulently used. At the end of prosecution, the accused was sentenced to a fine of 1000 penalty units that is GH₵12,000 (USD2,390) or in default 5 years' imprisonment.

Source: Ghana

Case Study 3: Credit / Debit Card Theft and Impersonation

A telephone company, in order to improve its services, opted for international transactions from a bank account to an electronic account. This innovation received a favourable response and allowed the company to record good results. However, it received an alert informing it that there were fraudulent international transactions, and that these were carried out from France to Cote d'Ivoire. The matter was reported to the agency responsible for the fight against cybercrime (PLCC) in order to apprehend those responsible. From the investigation opened following the report, it emerged that upon receipt of the illicit deposits, the beneficiary numbers immediately made the withdrawals.

The investigations conducted by the PLCC in collaboration with the Digital Forensic Laboratory (LCN) led to the discovery of the suspects through their cell numbers. The first suspect AAJ was arrested with the help of a unit of the said company. During interrogation, he admitted to having received several money deposits on his account from France. He went on to say that he was asked by one of his correspondents he met on Facebook to make withdrawals for ten percent (10%) of the amounts withdrawn. He ends by specifying that this correspondent Fabino did not give him any details, and that he just had to withdraw the money and give it to some family relation. Further investigations led to the arrest of Mr. Fabino at his home in Abidjan. The search led to the discovery of several credit/debit cards associated with banks from France, and not belonging to Fabino. Upon further interrogation, Fabino declared that he was responsible for making 16 deposits for a total amount of 2,290,344 FCFA, or 3,524 EURO while in France, to the numbers of his friend AAJ. Fabino was also, responsible for making several withdrawals that he made from the French bank account. The case is still ongoing at the time of reporting.

Source: Cote d'Ivoire

Typology 2: Email Compromise Scam / Fraud

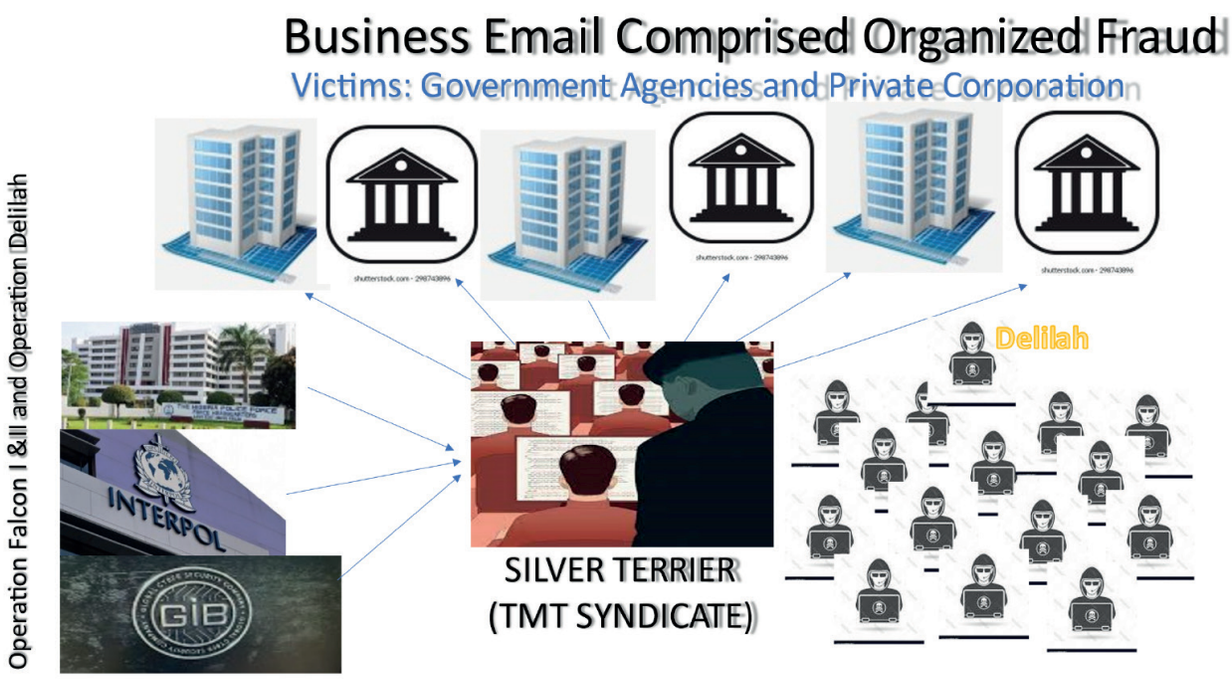
36. This typology has been in practice for a while and very popular in West Africa. The criminals used, engineering software to help them send spoof emails to potential victims around the world. Once, you click on those emails and/or start communicating with them, they can get access to sensitive information about your email and business, while using such information to defraud or scam you and the immediate members of your network.

Case 1: Business Email Compromise Organized Fraud

The Nigerian Police Force (NPF) arrested 11 alleged members of a prolific cybercrime network as part of a national police operation coordinated with INTERPOL. Arrested by officers of the NPF Cybercrime Police Unit and INTERPOL's National Central Bureau (NCB) in Nigeria, many of the suspects are thought to be members of "SilverTerrier," a network known for business email compromise (BEC) scams that have harmed thousands of companies globally. The

ten-day Operation Falcon II (13–22 December) saw 10 NFP officers deployed from the Abuja headquarters to Lagos and Asaba to arrest target suspects identified ahead of time with intelligence provided by INTERPOL. Field operations were preceded by an intelligence exchange and analysis phase, where Nigeria used INTERPOL's secure global police communications network, I-24/7, to work with police forces across the world also investigating BEC scams linked to Nigeria. The INTERPOL General Secretariat supported field operations 24/7, forensically extracting and analyzing data contained in the laptops and mobile phones seized by NPF during the arrests. This preliminary analysis indicates that the suspects' collective involvement in BEC criminal schemes may be associated with more than 50,000 targets. One of the arrested suspects was in possession of more than 800,000 potential victim domain credentials on his laptop. Another suspect had been monitoring conversations between 16 companies and their clients and diverting funds to "SilverTerrier" whenever company transactions were about to be made. Another individual was suspected of taking part in BEC crime across a wide range of West African countries, including Gambia, Ghana, and Nigeria.

Source: Nigeria



Methods and techniques

Developed domain names, phishing links, and massive mailing campaigns.
Developed/acquired malware / spyware programs and Remote Access tools.
Engaged in identity theft, impersonation, and document falsification.
Use of third-party businesses to move and divert funds extorted from victims.
The use of front businesses.

Red flags & Indicators

Unusual financial transactions.
Sudden change in lifestyle, from humble entrepreneur in a start up to living a flashy and luxurious.
Funds received in account with beneficiary name different from the account name.

Case 2: Phishing and Email Scam

Police investigation established that the complainant on December 1, 2021 Wawo-NGO email account at "wawoliberia@yahoo.com" was manipulated (phishing) and an impersonating malicious email, wawoliberian@yahoo.com ("n" was added to the original email) was allegedly used to communicate with her Donor "DED" and took away the sum of US$ 20,500.00 which was transferred through the Bank-B on November 15, 2021 from a donor partner DED and also used an orange number (0775000...) on WhatsApp in a conversation purporting to be the program officer of

the Wawo-NGO who introduced his/herself as finance officer and a Mobile phone number 0777028… assigned to a mobile money account username "BM-1" was attached to the Wawo-NGO email account which was subsequently removed after granting access to the email account of the Wawo-NGO. The technique used was hacking (Phishing) of email account and sending impersonating malicious email to donor for fund. A compromised email was allegedly used to request fund from donor "DED" and set up other communication links (WhatsApp) to authenticate transaction. The hacker was successful in the change of Bank-A bank account to Bank-B. The money laundering scheme in this case was Forgery and Theft of Property. The types of people Involved were Wawo-NGO staff and an unknown hacker. This case is being investigated since 28th December 2021.

Source: Liberia

Case 3: Business Email Compromise Fraud and Impersonation

The Nigeria Police Force Cybercrime Unit, domiciled with the INTERPOL National Central Bureau NCB Abuja, received a report from the German government through the office of the Attorney General and Minister of Justice, reporting a business email compromise fraud in connection with the procurement of COVID-19 protective masks. 'Unidentified fraudsters gained the trust of an intermediary in Ireland by initiating business transactions involving medical products. By skilfully negotiating with the intermediary and presenting counterfeit delivery contracts and invoices, the fraudsters made the intermediary believe that he would be able to deliver large quantities of COVID-19 protective masks for the German government authority. In the end, down payments in the amount of more than EUR 2.3 million were made to a bank account in the Netherlands, and partial payments of EUR 498,000 had already been transferred to a first-generation bank account in Nigeria on the instruction of a Nigerian, Babatunde Adesanya alias Teddy A, who gave in advance instructions on what to do with the money. Musterpoint Investment Nig Ltd., a company domiciled with a first-generation bank in Nigeria, was the destination of the said EUR 498,000. However, because of international law enforcement cooperation upon receipt of the report, the bank was contacted by INTERPOL and the transfer was stopped, with the money returned to its sending point. This led to the arrest of two suspects by the Nigeria Police Force Cybercrime Unit, who are now facing prosecution at the Federal High Court of Nigeria.

Source: Nigeria

Case 4: Business Email compromise Fraud

On February 5 and 12, 2018, a commercial bank made two transfers respectively of 50,000 Euros and 145,000 Euros in favour of two (02) companies. These transfers were deemed to have been authorised by one of its customers who has an online banking agreement with the bank and has always instructed its transfers by email. The bank received the instructions by email for the two transfers in question and received another email by which the client changed the bank details of the beneficiaries. The various Swifts of the two transfers were produced and sent to him after execution. The transfers were not disputed until 02/20/2018 when the real client came back to say that although he authorised the transfers, he was however, did not give any instruction to modify the details of the recipients of the transfer funds. The bank later discovered that a cybercriminal was able to access the banks system and introduced those modification of recipients with fake emails into the transfer process. The case is still ongoing at the time of reporting).

Source: Togo

Case 5: Business Email compromise Fraud

The FIU received a report of identity theft fraud from Hibiscus, a local NPO. They were expecting their second disbursement of funds totalling NLe707,841.12 meant for key affected populations in the interior from their international partners, Gardenia Help. The funds were fraudulently diverted into another account bearing the same name Hibiscus at another Bank WY. Hibiscus' internal investigations revealed that the Programme Manager's email had been hacked and was the major conduit for flow of relevant information between the fraudsters and the international partners. Hibiscus's activities had now been suspended by Gardenia until the matter was resolved.

The FIU's investigations revealed that a fraudulent Hibiscus account was indeed opened at Bank WY and the funds totalling NLe707,841.12 were indeed transferred directly from Gardenia Help.

The funds were immediately transferred to another account Sunflower Tech within the same bank and withdrawn within three days by the sole signatory of Sunflower Tech. Investigations also revealed that there was a direct connection between the fraudulent Hibiscus NPO, Sunflower Tech and its signatory. Bank WY failed to conduct proper due diligence and KYC measures on the opening of the fraudulent Hibiscus Account. If they had, they would have detected all the glaring red flags. They were more concerned with profitability.

Gardenia Help NGO and Hibiscus NPO have very limited knowledge in money laundering and terrorist financing rendering their internal systems porous and easily susceptible to fraudsters within their organisations. The ultimate beneficiary has been apprehended by the ACC and the investigations is ongoing.

Source: Sierra Leone

Typology 3: Hacking and Defrauding Business / Organisation's Systems (Website/Database)

37. Another popular typology is hacking and taking over the website or platform / database of business and organisations using very sophisticated engineering techniques and software. The techniques are not very much different from Malware or Ransomware attacks. However, in West Africa, the criminals hardly disclose themselves asking for ransom. They are either paid to do so by rivals or competitors or in the case of financial institutions, the platform where transactions are done is taken over to execute illegal transfers and payments before the victims can detect and make effort to regain control of their system. There are times when insider dealings is part of the modus operandum.

Case 1: Hacking Business / Organization System (DDOS & defrauding)

A British cybercriminal, Mr. Kaye attacked a Liberian GSM company and inadvertently crashing Liberia's internet - in 2016. Kaye, from Egham in Surrey, is a self-taught hacker who began selling his considerable skills on the dark web - offering individuals opportunities to target and destroy their business rivals. According to court papers, Kaye was hired in 2015 to attack a leading mobile phone and internet provider company, by an individual working for its rival and main competitor. There was no suggestion that the rival company was aware of the employee's action - but the individual offered Kaye up to $10,000 (£7,800) a month to use his skills to destroy the company and bring it services under disrepute and cause reputation damage.

Mobile phone users began to see their devices go offline. The company called in cyber security consultants who attempted to repel the attack, but by that point it was too late because the botnet ran out of control. Liberia's internet was dependent on both a small number of providers and a relatively limited Atlantic cable. Kaye had sent so much traffic at company, causing the entire national cyber system to jam. According to investigators, the country's internet repeatedly failed between 3 November and 4 November 2016 - disrupting not just company that was attacked, but organisations and small businesses and individual users throughout the country. In turn, Mr Kaye's actions prevented the company's customers from communicating with each other, obtaining access to essential services and carrying out their day-to-day business activities. A substantial number of customers switched to the main competitor.

Kaye admitted to charges on an offence of computer misuse, launching cyber-attacks against a company in Liberia, and for being in possession of the proceeds of crime - relating to $10,000 found on him when he was arrested. In the years preceding the Distributed Denial of Service (DDOS) attacks, the company annual revenue exceeded $80m (£62.4m). Post attack revenue recorded a decrease in tens of millions and increasing the company's liabilities then, also in tens of millions of US dollars.

Source: Liberia

Case 2: Hacking Business / Organization System (DDOS & defrauding)

In 2020, a financial institution reported to the police that cybercriminals compromised their entire banking system and had full access to their core banking system. The cybercriminals modified passed transaction reference numbers and injected a total sum of D48,000,000 (USD 857,142.8) into different accounts. The hackers also lifted the bank's ATM daily withdrawal limit and thus allowing those account holders (local actors/conspirators/accomplices) to withdraw as much as possible. The hackers run queries on the banking system and delete all the illegal transaction histories as a result the transactions on the affected accounts could not be viewed using the bank front end but could only be viewed from the Gam switch Sarver at the central bank.

The account holder (local actors/conspirators/accomplices) succeeded in withdrawing (using ATM) D7, 000,000 (USD 125,000) and further investigation revealed that part of the money was sent to Ghana, South Africa, and Senegal. However, through international co-operation (Interpol and FIU), part of the funds sent to Ghana was recovered from a company account and all the funds sent to Senegal was also recovered.

Also, it is important to acknowledge that at the time of this investigation, the country had no digital forensic lab to examine devices. Even though none of the hackers were arrested, 23 suspects, who were accomplices/conspirators to the hackers, were arrested. The investigation was concluded, and the case was sent to the Attorney General chambers for advice.

Source: The Gambia

Case 3: Hacking Business / Organization System (DDOS & defrauding)

During July 2020, the Central Brigade for the Fight against Cybercrime received an instruction by way of a letter sent by the Prosecutor of the 1st High Court of Ouagadougou, to carry out a detailed investigation on fraudulent access and obstruction of the operation of a computer system, modification of computer data, association or agreement to commit computer offences, theft of cash, money laundering and to proffer charges against any person involved in the above mentioned offenses.

The investigation revealed that on the night of Sunday June 21 to Monday June 22, 2020, hackers attacked a mobile money electronic platform through a telephone network. They attacked five (05) main accounts of the platform and that of a local bank where the mobile money platform was housed and managed. The hackers carried out fraudulent transfers for a total amount of ninety -nine million one hundred and eighty-seven thousand five hundred and seventy-nine (99,187,579) FCFA. These transfers were made to several telephone numbers, holders of mobile money accounts in the country and to other numbers in 3 other neighbouring countries. The total sum of money in the accounts that the hackers were able to block both national and international, was more than three hundred and eighty-one million (381,000,000) FCFA.

The investigation made it possible to arrest several suspects and were taken to the prosecutor of the 1st High Court for further action.

Source: Burkina Faso

Case 4: Laundering (Layering) through a Compromised Bank Employee

From the 20th to the 29th of September 2022, a commercial bank in Bissau reported that some fraudulent online transfer operations were carried out by unknown individuals and were not employees of the bank. According to sources from the FIU and Police, transfers were made from the bank's own account to customers' accounts in the same bank.

Following the investigation, the Judiciary Police with the help of the Criminal Conduct and Scam unit and the National Unit for Combatting Economic Crimes, requested the cooperation of the telecom companies to track communications made in the past one month, using certain (6 SIM numbers) suspected mobile phones to have been involved in the case. Mrs. Y, the 1st suspect cooperated with Police on her involvement on the criminal conduct of fraud and breach of trust.

Mrs. Y confessed that she is the holder of a saving account domiciled at Bank XPTO in Bissau, however, at the request of her husband Mr. X, to provide her account number to a friend Mario, who needed an account linked to a VISA card at Bank XPTO. Without any due diligence, Mr. X provided the account details to his friend Mario. Few days later, Mrs Y alluded that she received a message on her cell phone indicating a credit operation in the amount of six hundred and forty-eight thousand, one hundred and forty-one CFA francs (648,141 CFAF). She later made her VISA debit card available to her husband, who through his friend, collected the money in instalments.

And days later, the account was again credited with the sum of Five million CFA francs (5,000,000 CFAF). This time her husband's friend asked her to go to the bank counter to make a direct withdrawal, which should be through advance notice, but due to her husband's relationship with one of the employees, she was able to withdraw the full amount at once. She later received a call from KP, who asked her to return to the bank in order to clarify the situation surrounding the undue withdrawal she made and abnormalities that have occurred in her account.

The investigation is still ongoing. However, it is worth noting the existence of failures in the electronic money transfer control system at the referenced bank and which cyber criminals in collaboration with certain bank employees have capitalised on to carry out illegal transfers outside the normal operation of the bank. The case also, revealed the vulnerabilities of the control system at the level of banks and financial establishments, as well as the threats of cybercrime that country is facing, particularly, in the absence of the infrastructure and technical capacities to face up to these threats.

Source: Guinea Bissau

Case 5: Hacking Social Media Account, Impersonating and Defrauding

A victim Mary T. reported to the police that someone impersonated to be her uncle through her Facebook messenger account asked to transfer US$800.00 and LR$75,000.00 to a given number on May 11, 2022. The hacker created a Facebook messenger account using her uncle's full name. The idea was that the uncle is in urgent need of money to settle some obligations in Liberia and the money will be refund to her afterwards. After being convinced and based on the trust for her uncle, she made a transfer of the amount via MoneyGram from the USA as instructed. The criminal after hacking the victim's relative messenger account and impersonating as the uncle, requesting money transfer and sending message instructing victim to transfer money to a given number. The predicate crimes to money laundering are fraud and extorsion / theft of property perpetrated by an individual and an unknown hacker. In this case, the victim received message purporting to be from her uncle to transfer funds to mobile money account. The case is being investigated.

Source: Liberia

Case 6: Insider Dealing, Organized and Fraudulent Credit Facility Scheme

The FIU received a report (Fraud-Return Investigation) on a Suspicious Unauthorized Credit Disbursement from Jimpex Commercial Bank (JCB). 150 customers of JCB were fraudulently granted overdraft facilities with no documentation to the tune of Le54,484,754,082.47 (0.5 million US dollars).

JCB's Portfolio Reporting Officer and the Acting Divisional Head (Credit Risk Management) were the masterminds that hatched up the illegal scheme. They then involved into the scheme IT personnel who had access to the data.

The Credit Risk Manager used his special access code to authorize overdrafts to pre-selected customers of JCB. The Credit Risk Manager carefully selected existing customers of the bank who were operating credible businesses and enticed them to engage in the illegal scheme. Each of the beneficiaries of the illegal scheme was requested to provide a specified amount in cash to the conspirators before they could gain access to the illegal overdraft facility. Upon payment of the requested amount the Credit Risk Manager authorized the overdraft facility by using his access code. The ICT personnel that was part of the scheme also turned a blind eye.

TOCU's investigation has linked 4 newly constructed ultra-modern houses and a fleet of luxury cars to the credit risk manager and the portfolio reporting officer. The credit risk manager is on the run while investigations is ongoing.

Source: Sierra Leone

Typology 4: Advance Fee Fraud and Money Laundering

38. This is still the most committed cyber enable predicate offence in West Africa. Its account for more than 40% of the submitted cases here reported. The advance fee is either based on romance scam, sextortion, inheritance claims or business proposals, or a combination of two or more of the methods mentioned. Another unique method worth highlighting is advance fee fraud conducted from behind prison bars, with prison officials as accomplice.

Case 1: Gold Scam and Advance Fee Fraud

This case was investigated by the Police based on a complaint filed by two British businessmen. The two investors from the United Kingdom and their business partners were in 2020 introduced by an online acquaintance to Mr. 'A', a Ghanaian, as a businessman who traded in gold. The investors expressed interest in buying gold bars from Mr. 'A' and subsequently travelled to Ghana, on Mr. A's invitation, who also demanded they meet him in person for negotiation in respect of the transaction. In February 2020, Mr. 'A' and an accomplice, Mr. B met the investors and showed them 20 kilogrammes of gold bars.

The foreign investors expressed their readiness to buy five kilogrammes of the gold, for which Mr. 'A' and his accomplice demanded and collected $69,000 as initial part payment of the value of the gold. After receipt of the money, they promised to export the gold to the investors, who would take delivery of it in Dubai in the United Arab Emirates. But they ended up exporting only one kilogramme of gold to the investors. Mr.' A' explained that he could not export the appropriate quantity of gold because of delays in the documentation process by Customs officials at the Kotoka International Airport and promised to export the remaining quantity to the investors on December 3, 2020, but failed to do so. He later requested for $130,000, being the outstanding payment for the four kilogrammes of gold and requested for another $70,000 from the investors to guarantee the export of the rest of the gold. When he failed to honour his word, he indicated that he had been unable to export the gold, as there were no airlines to export the gold due to the COVID-19 pandemic.

Mr. A also claimed the waybill to facilitate the export of the gold could not be accepted by the Precious Minerals Marketing Company, as the quantity was too small, so he would add five additional kilogrammes of gold to bring the total to 10 kilogrammes for easy export. In July, 2020, Mr. A told the investors he had been arrested by INTERPOL and officials of some security agencies and the gold bars had been confiscated.

To facilitate the release of the gold, he demanded various amounts of money and later indicated that the gold bars had been released to the Economic and Organised Crimes Office (EOCO), which was demanding $300,000 before releasing the precious mineral to him. The investors sent the $300,000 to Mr. A, bringing the total amount sent to him to $1,075,000, but he failed to fulfil his promise, leading to his arrest. He was then charged with conspiracy to defraud by false pretences, defrauding by false pretences and selling and buying minerals without licence. The trial is currently on-going.

Source: Ghana

Case 2: Sextortion, Child Pornography and Extorsion

In 2016, a case was reported to the police on three individuals: Flavio, Filipe and Steve. The suspects created a fake profile on social media by the name of "Maurice Marcovich", being used for criminal purposes. They used the fake page to send friend request to their potential victims who were mostly minors at the time of the crime. After exchanging a couple of chat messages via Facebook Messenger, they started threatening the lives of the victims, their families and/or loved ones if they do not show themselves in pornographic poses, taking photographs and videos with their own mobile phones and forcing them to send them through the Messenger.

Having seen the photographs and footage of the victims during the talks via chat on Internet –Messenger, the "fake profile" under the name of "Maurice Marcovich", orders them to send a friend request to "Flávio Yolo Alves", "Rui Filipe Alves" and "Steve Aristides Santos", at Facebook.

Still, through this ruse, they frightened and coerced the victims, to meet with them and practice sexual acts, filming with their cell phones, and with those of the victims, which they accepted due to the fear that they instilled in them, either through threats or through the public disclosure of their pornographic photographs and videos that they already possessed.

Victims were threatened, not only with the publication of photographs and videos, but also with the sending of a picture of a firearm to be loaded and together with the following messages: "you are not going to ignore me anymore", "I kill all the days", "I know a lot about you", "because I want your blood", "tomorrow you can be sure you won't have life", "I am an international drug dealer in Syria, Brazil and France", "and I have already ordered the killing of several students in Iraq" sic. They also sent the victims photographs of their relatives, which they captured in public places and close to their homes, to intimidate and frighten them even more.

Faced with these insistent death threats, the victims, desperate and afraid, acceded to the pretensions of these individuals, and sent more photographs and videos, obscene and indecent, showing their private parts as well as their faces. .

These individuals, sometimes individually or in groups, arranged to meet the victims in different places, and forced them to have sex with them, and the acts were filmed and photographed, claiming that they had orders from "Maurice Marcovich" to do all that and send it.

In the course of these violent acts against these victims, one of them, under the age of 13, became pregnant, and evidence collected later, which was based on the collection of the suspects' DNA for the purpose of identifying paternity, proved that "Rui Filipe Alves" was the father.

Dissatisfied with the actions above, they are still under constant threat, using the false profile "Maurice Marcovich", forced some victims to prostitute themselves and, as a result, received the money from this practice, which they charged each client, an amount between 5 and 7 thousand escudos, approximately 50 to 70 Euros/Dollars.

The individuals "Flávio Yolo Alves" and "Rui Filipe Alves" were arrested and presented to the Court and when judged, Flávio was sentenced to 33 years in prison and Rui to 14 years.

Source: Cabo Verde

Case 3: Use of Fictitious / Shell company and Advance Fee Fraud

In 2009, Mr. A, who is a merchant, opens an account in bank X for reasons related to his commercial activities. But on this account, he only receives transfers from abroad. Four years later (2013), his wife opened an account in the same bank, again for business reasons. The latter's account received over the period from 2013 to 2019, 48 transfers for a total of122 282 518 FCFA. Only one payment transaction has been made on the account. But surprisingly, Mr. A controls his wife's account in its entirety. All withdrawals were made by himself and generally immediately after each reception. In 2014, he incorporated and opened a third account in the same banking institution. Under the same conditions, he benefits from 114,905,014 FCFA between 2014 and 2019. All these facts have led bank X to make a suspicious transaction report to CENTIF. In 2018, he opened another account in a second bank Y and received a transfer from a Nigerien bank, for a total amount of 189,500,000 FCFA which turned out to be a fraudulent transfer obtained from an attack on the bank's computer system. But thanks to the vigilance of the latter, the funds could be returned to so much before Mr. X came into possession of the sums. Bank Y immediately sends a DOS to CENTIF. CENTIF's investigations revealed that Mr. X is the little brother of a cyber crook known to his databases. he is part of a network of cyber criminals who engage in Nigerian-style scams (scam 419). Their method is the use of shell companies and intermediaries or nominees to lure their victims by offering them very lucrative deals. Along the way, they create imaginary costs that the victim must pay, in particular the costs of studying the file, legal fees, accounting fees, etc. This ride allowed them to extract 451,615,304 CFA from their victim. Following the investigations, Mr. X was found guilty of money laundering, organized fraud and breach of computer security and sentenced to 72 months in prison, 12 of which were suspended, and a fine of 100,000,000 CFA. His wife was convicted of simple BC, sentencing her to 36 months in prison, 12 of which were suspended and a fine of 50,000,000 CFA. There was confiscation of 11,481,787 FCFA seized on one of their accounts and confiscation of a car belonging to them for the benefit of the State.

Source: Togo

Case 4: Romance Scam and Advance Fee Fraud

Mr. A, a Ghanaian citizen who, who posed as a woman to defraud a 43-year-old Australian national, Mr X, in a romance scam, has been sentenced to 10 years' imprisonment. In his dealings with the victim, Mr. A posed as a female with a fake identity online and met the victim on a dating site. The victim is a retired commercial fisherman and a citizen of Australia. The victim indicated that after getting involved with the scammer online, Mr. A convinced him to buy property in Ghana and to also support the supposed family of Mr. A financially. As a result, he remitted a total amount of $115,000 AUS to the accused in Ghana via bank transfers.

The victim realizing that he was being defrauded, filed a complaint with EOCO and requested EOCO to conduct investigations into the alleged scam. The accused was apprehended in December 2017 and was subsequently arraigned before the High Court on the charges of defrauding by false pretences, money laundering and possession of forged documents. In June 2018, the accused was found guilty of the charges and sentenced to 10years imprisonment with hard labour. An amount of GHS52000 (USD11,000) outstanding in his account was frozen and remitted to the victim.

Source: Ghana

Case 5: Job Recruitment Scam and Advance Fee Fraud

In 2022, the investigations in this case originated from several complaints made to the criminal police bodies (OPC), the Judiciary Police and the National Police, where some victims report that they received an invitation via social network. FACEBOOK, of a profile with a photograph of the Minister of Foreign Affairs and Communities of Cape Verde, and others say they received an invitation from a profile of the Deputy Minister of the Prime Minister and Minister of Finance to which they accepted thinking it was about these gentlemen.

That after the friend request was accepted, the people on the profiles began to exchange messages written in Portuguese, through the Messenger, and during the conversation, he promises them a job offer at the United Nations (UN), as a diplomat representative of Cape Verde, whose salary would be approximately five thousand dollars per month (approximately 500,000$00 thousand Cape Verdean escudos) with taking into account that the minimum salary in CV is 13,000$00 thousand escudos (130 Dollars USD).

Having made this promise of work and accepted by the victims, the person in the profiles provides them with a contact that he claims to be a UN official, with whom they, the victims, should start talking to deal with matters related to being hired for the position.

Usually, this contact is a number in the WhatsApp, and the victims begin to talk to the person who, in all reported cases, said it was a man's voice. The person asks them to send documents, such as a copy of the passport, curriculum vitae, criminal record, and the money via a transfer to pay the costs of processing the documents (employment contracts, identification badge as a UN employee, etc.,).

Victims send the requested sums via Western Union or Money Gram, amounts of approximately 100,000 escudos (1000 Euros), but days later, that person contacts them again to ask for more money for the hiring process, and, to give more credibility, they send a work contract that must be signed and sent via email. Once the contract is signed and sent, they again ask for more amounts, with other justifications. However, if the victim proves unable to pay, they threaten to void the contract.

Once the victims are in despair, when they are no longer able to pay, they go to the Minister in person or do it through third parties known to the Minister and, this is how they are clarified that they have entered into a scheme where they were deceived by cyber criminals, therefore, the profiles do not belong to the Ministers. In other words, they are fake.

In relation to the facts exposed above, in which there are seven (07) victims, the cybercriminals had an income in the total amount of3,387,730$00 ECV, corresponding to (USD 31,709.2). However, all money was sent via Western Union, for Benin, specifically Cotonou.

Source: Cabo Verde

Case 6: Business Proposal Scam and Advance Fee Fraud

On December 3, 2018, CENTIF-TOGO received a suspicious transaction report from a financial institution A following several transfers of funds received from abroad by Mr. KM. At the opening of the account, he declared to be the manager of the company ES whose activity is the import-export of shoes and bags. For a company whose vocation is import and export, funds should normally be sent from Togo to foreign countries to purchase goods, but not only has the account never been transferred to Abroad, it has functioned more like a bounce account, where the funds from the transfers received are immediately withdrawn, leaving the account dormant until a new transfer is received. This falls within the atypical case of a cyber fraud scheme of the 419-type scam. CENTIF's investigations revealed that he has another account at the level of a financial institution B and whose operation is identical to that of the account of institution A. On June 18, 2021, CENTIF-TG received information sharing from its counterpart in Japan concerning Mr. KM, for the facts of attempted fraud through a fraudulent transfer. Indeed, on December 25, 2020, a Japanese national Mr. JJ presented himself at the counters of a bank in his country and insisted on the fact that he had 3,300,000 USD or approximately 1,980,000,000 FCFA in his bank account in Togo. This account turns out to be account B of M KM. Mr. JJ then asks his bank to transfer 400 USD to the said account to carry out formalities to recover the 1,980,000,000 FCFA available there. The Japanese financial institution refused to execute the transfer order for doubts it had on the reason for the transfer and filed an STR to the financial intelligence unit of Japan which in turn reported the case to CENTIF TOGO. However, the victim, allowed himself to be extorted between 2015 and 2021, and made 41 transfers of funds received, at least 37,598,670 FCFA.

Source: Togo

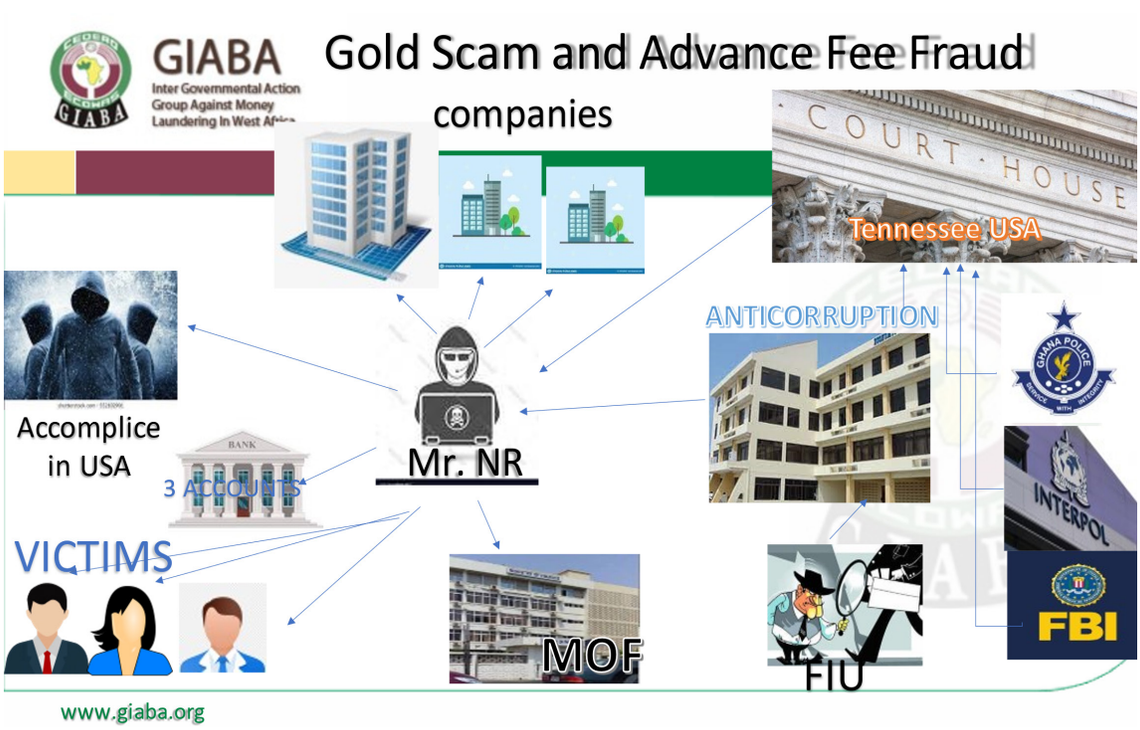
Case 7: Romance / Gold Scam and Advance Fee Fraud

Case Study 2. An intelligence was sent by FIC to EOCO on the activities of a Nigerian National resident in Ghana who owned and operated a company which had its nature of business as maritime, bunkering, shipping, and construction. He came to the attention of the Financial Intelligence Centre (FIC) when he received some inflows from the USA. When he was initially queried about the inflows, he averred that he was about setting up a bank and was in the process of obtaining approval from the Bank of Ghana. In August 2016 he received additional inflows which totalled US$ 330,749.47 from three sources, one corporate institution in the USA and two American citizens. His bank account was immediately frozen by EOCO, and investigation was initiated. During investigation it was established that he misrepresented himself to some of the victims he met on the dating site www.match.com as a white male working on projects in Ghana, with fake aliases. He also misrepresented himself as a gold dealer trading under the company name of two fake companies which allegedly had gold worth US$8 million. He also presented fake documents purporting to have emanated from the Ministry of Finance as evidence of his purported gold being held at the Ministry.

In August 2017, while the investigation was ongoing in Ghana, a federal grand jury in the U.S. District Court for the Western District of Tennessee indicted the suspect and others for conspiracy to commit wire fraud, conspiracy to commit money laundering, conspiracy to commit computer fraud and aggravated identity theft. The federal court indicated that the suspect in collaboration with other co-conspirators in the USA deployed sophisticated anonymization techniques, including the use of spoofed email addresses and Virtual Private Networks, the co-conspirators identified large financial transactions, initiated fraudulent email correspondence with relevant business parties and then redirected closing funds. The victims were identified to be from USA, Australia, UK, and Finland.

He was extradited to the USA in December 2019 and was sentenced to 3.5 years in prison on June 16, 2021. The investigation had collaborations from FIC, Ghana Police Service, Interpol and the FBI at all levels leading to a successful investigation and prosecution. No connection to terrorism financing was identified. EOCO in June 2022 has commenced action at the court to repatriate the proceeds of the crime, which have been frozen in the various bank accounts, to the USA.

Source: Ghana



Methods and techniques

- Exploring popular dating site using fake identity
- Building online / distance relationship and building trust to lure victims
- Using third-party professionals, particularly legal persons
- The use of front businesses

Red flags & Indicators

- Unusual financial transactions
- Inconsistencies in statements during law enforcement interrogation
- Funds received in account with beneficiary name different from the account name

Case 8: Trade (Import/Export) Contract Scam and Advance Fee Fraud

XZ, residing in Niamey, received a telephone call (GSM) from a number, with a code for France. His interlocutor on the phone, introducing himself as GMN, had collected enough specific information about him to the point that XZ believed that GMN had known him since. GMN manages to establish and gain through well-oiled social engineering the trust of XZ. GMN offered XZ a deal to deliver one of the moringa sap. GMN explained to XZ that he had such a business relationship with a well-known but deceased personality. XZ is therefore chosen to replace this one, explained GMN to him, specifying the desired quantity. GMN explained to XZ that moringa sap is a very popular product that he is researching on behalf of a doctor working for a laboratory based in France at Carrefour KYC.

GMN communicated to XZ the name of Kaboré Elh Moussa, domiciled in Ouagadougou, as well as the telephone number of BBP from which Kaboré and GMN claimed to obtain supplies of moringa sap in the past. XZ is informed that he must contact BBP to ask him if he still has moringa sap in quantity and quality and at the same time inquire about the price.

After XZ and BBP had agreed on the quantity available as well as the price, BBP offered XZ to receive a first sample first. This sample is delivered directly to Niamey by a person presented as the son of BBP who personally receives the costs relating to the price of the sample. The sample was submitted to the expertise of AC, a European whose telephone number had been provided to XZ by Kaboré Elh Moussa. Once the quality was confirmed by AC, XZ and BBP agreed on the delivery conditions (costs, transport methods, etc.) for the entire order. For this, several additional costs are requested from XZ depending on the nature of the goods. These are the costs of packaging, packaging, phytosanitary, and administrative formalities including customs.

After all these charges, including the purchase price of the bulk order and other additional charges, XZ anxiously waiting for the Moringa sap to be delivered to him, tried in vain to reach GMN, Kaboré, BBP, AC and the alleged son from BBP. Everyone had turned off their cell phones.

Mechanism, Instrument and Technique of BC identified in the case

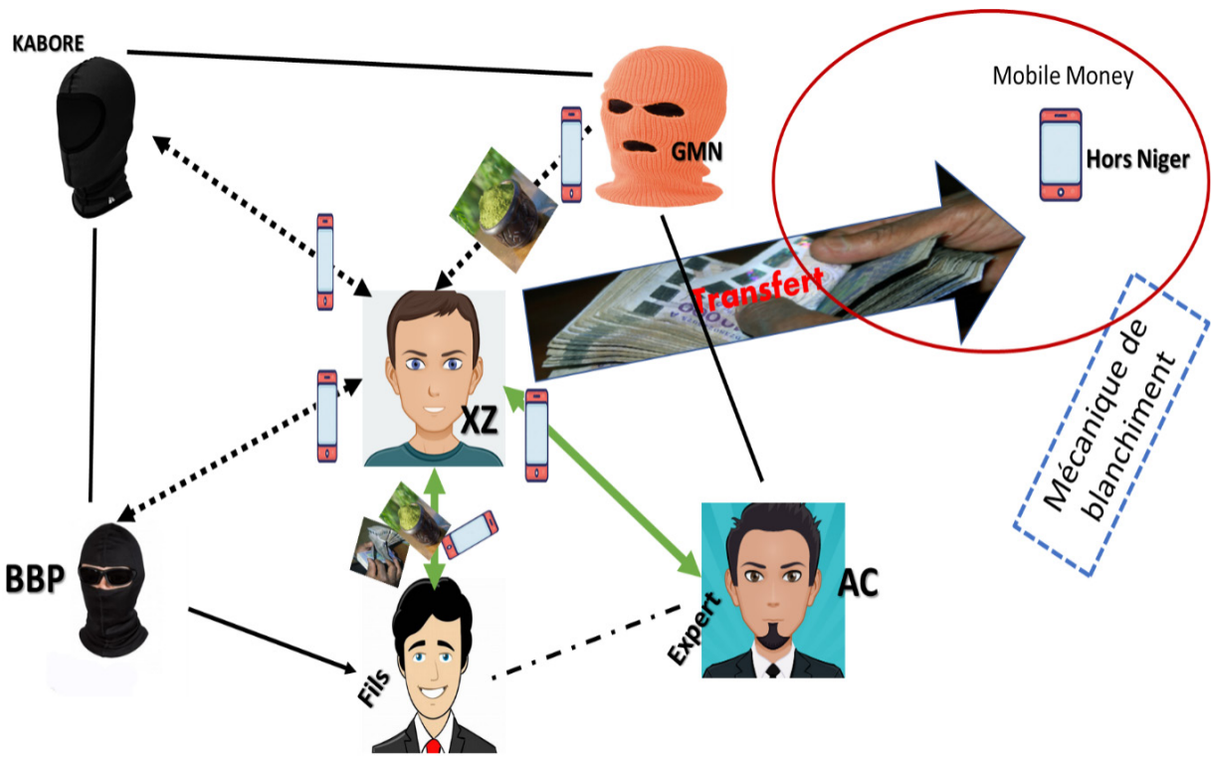
From the negotiation and the remittance of funds, XZ had physically met only two (02) people: the alleged son of BBP who delivers the sample to him for analysis and the expert AC in charge of analyzing the said sample. All the fraudulent maneuvers that took away the will of XZ to hand over its funds were only possible thanks to a well-known method in cybercrime: social engineering via ICT.

The predicate offense of electronic communication fraud generated funds that wereplaced away amechanism what is mobile money and have started astacking process (outward transfer) by the same mechanism (mobile money application)

At the time of their arrests, the suspects were found in possession of compromising objects such as mobile phones, SIM cards, receipts for transfer of funds, false identity documents used for withdrawals, as well as bags containing black seeds.

The suspects were referred to the prosecution for fraud by an electronic means of communication without having been instructed by the OPJ on the ground of the BCFT.

Source: Niger



Case 9: International Trade Freight Services Scam and Advance Fee Fraud

This case commenced in early 2012 when the accused came under the radar of FIC for suspected illicit inflows received into his bank accounts. The accused went into hibernation when his account was frozen and later resurfaced in 2016 with multiple identities. The accused used three different passports bearing different names to open and operate seven accounts at different branches of Bank "A". Accused also had accounts with four other banks which he opened using fake documents such as forged Passport and Voters ID. The accused then fraudulently misrepresented himself as a businessman online to his victims using the names George Hanson and Daniel Brown who was into international freight forwarding services across the world. The scheme is structured such that his services are recommended by supposed customers (his co-conspirators) of victims (prospective clients) mostly from US, UK and other countries like Australia who end up making advance payments for his services. He received over 20 remittances totalling USD351,000 and additional GBP40,000 in his multiple accounts from the victims.

Investigation established that the accused used part of the proceeds of his crime to procure a house in Ghana. He spent part of the cash and had a balance of GBP10,000 in his account which was frozen during the investigation. He was charged for money laundering, defrauding by false pretences, tax evasion, impersonation, and forgery of documents among others. In court, even though the accused pleaded not guilty to all the charges, but the court found him guilty and sentenced him to two years' imprisonment and a fine of three thousand penalty units, or in default an additional three years, on charges of forgery after the prosecution had proved its case. On charges of money laundering, accused was found guilty and sentenced to a term of two years and a fine of four thousand penalty units or in default, four years in hard labour. The court also ordered the forfeiture of all funds of the accused, and landed property including house acquired was forfeited to the state in addition to the GBP10,000 outstanding in his bank account.

Source: Ghana

Case 10: Romance / Inheritance Scam and Advance Fee Fraud

Case Study 1 (Romance and inheritance Scam Case)

The accused was arrested for being involved in a grand scheme to defraud a resident of New York, United States to the tune of USD700,000. The accused (a male), using a fake female identity (Miss X), initiated an online romantic relationship with the victim. The accused procured the services of a popular porn actress, Miss Y, resident in America, who misrepresented herself as Miss X to make the relationship look real. The porn actress convinced the victim about a gold inheritance she had in Ghana and both came to Ghana. In Ghana, they met a taxi driver called "Z", who turned out to be the accused and the mastermind. Miss X presented fake documents to the victim showing that she inherited a Gold Mine by name Company A and wanted to transfer same into the joint names of her and the victim. Consequently, the victim transferred a total amount of USD428,865 into bank accounts of a company which turned out to be owned by the accused and another USD349,993 to a real estate company on the instruction of the accused as payments for gold. During investigation, the real estate company which received USD349,993 contended that the accused contracted them to design and build a mansion for him in a particular prime area in Accra, Ghana. From the same fraudulent enterprise, the accused built and furnished a 3-bedroom mansion for his father, and also acquired a private vehicle - Hyundai Tucson.

The accused was charged for money laundering, impersonation, defrauding by false pretences, forgery of documents and was arraigned before the High Court – Financial Crime Division. In August 2020 while the prosecution was on-going, the Court was notified about the death of the accused. The Court ordered for the assets of the accused to be frozen, and an Administrator-General was appointed to oversee the estate of the accused, in line with the Administration of Estates Act, 1961 upon an application from EOCO. The accused's father instituted an action to dismiss the motion against the accused, that since the originating motion was brought against the accused, who was deceased, same is incompetent and should be dismissed. However, the case was assessed in the light of Section 50 of the Economic and Organised Crimes Act, which empowers the Court to confiscate tainted property if the person from whom the property was seized dies or absconds hence the court found for EOCO.

Source: Ghana

Case 11: Romance Scam and Advance Fee Fraud

The NFIU received a suspicious transaction filed by a reporting entity involving multiple high-volume transactions up to the tune of NGN 4,981,206.32. The funds were received by one Mr. X between July 2 and August 17, 2020, in 10 transactions via Western Union Money Transfer. Transactions were sent in from Canada by Mrs. Y with no justification or evidence of a family relationship. The high-volume transactions are a red flag, as is the split pattern of the transactions to avoid the threshold limit. The recipient's location and age also arouse suspicion of a romance scam. The case was forwarded to the relevant law enforcement agency and is currently being investigated for Romance scam, advance fee fraud and money laundering.

Source: Nigeria

Case 12: Romance Scam / False Pretence and Advance Fee Fraud

This case was reported to the police in 2022, and suspect/s were believed to be living in Nigeria. They have opened several accounts using fake names and pictures of beautiful white ladies and subsequently lure men into an online relationship. In the process, they will make their victims believe that they need to prepare a certain document called 'affidavit of trust for long distance relationship'. In their quest to get this document, the victims would be referred to a purported lawyer believed to be part of the criminal syndicate who will extort money from the victims in the name of providing this document.

Investigation established that the aforesaid suspects were able to scam their victims with a sum of D587, 700.00 (five hundred eighty-seven thousand, seven hundred dalasis) (USD 10,494.6) that has been remitted to the bank accounts in Nigeria.

That a correspondence letter was sent to Interpol Nigeria in a bid to locate the suspect and possible recovery of the money obtained illegally from his victims, but no response has been received so far.

Source: The Gambia

Case 13: Human Trafficking, Kidnapping, Sextortion, and Extortion

In a case handled by the DSC, a cybercriminal network leader, taking advantage of the difficult living situation of two young Nigerian girls, brought them to Senegal, under the pretext that he was able to find them jobs.

Once in Dakar, he confiscated their travel documents, tested them for HIV and AIDS, and then forced them into a form of sexual slavery under penalty of death.

He photographed the girls naked and used the images as bait for his victims in his cybercriminal activities.

He would also force them to sleep with Europeans whom he would invite to Senegal, kidnap and release after their parents paid a ransom.

His modus operandi consisted in contacting his prey by Messenger, presenting himself with profiles of young girls. Thereupon, he used them to communicate via WhatsApp with the victims to reassure them. It is on the basis of these manoeuvrers that they managed to attract five (05) European nationals, who were sequestered and released after paying ransoms.

This highly structured network had branches in the sub-region where some members of the group were in charge of cashing the funds from their activities that they transferred via electronic transfer systems.

In order to recover the money transferred as a result of the blackmail, the leader of the gang cooperated with certain money transfer agency officials who handed over the funds despite the normal procedure.

Source: Senegal

Case 14: Fraud, Blackmail, Extortion and Money Laundering

In 2022, the MSD apprentice driver from the city of Koundara in Guinea, back in his hometown, after a long stay in a neighboring country of Guinea, decided to embark on cybercriminal activities to support himself. He created a Facebook account and pretended to be a woman named AB for the purposes of the cause, he uploaded several photos of a woman with attractive physical fitness from an Instagram account and sent invitations to several mature men who responded to said requests.

Thus, began between MSD acting under the identity of AB and its victims, intimate conversations during which they proposed to the latter to maintain carnal relations by video call mode and managed to film his victims, whom he then blackmailed by threatening to pay between 5,000 and 10,000 US dollars per month or risk of seeing their nudities exposed on social media networks.

The victims were generally respectable men, so they paid him the required amounts. The various amounts raised were used by the cybercriminal to set up several projects: the purchase of a mini bus for public transport, a car for his personal trip and finally the construction of a video club and a bar. These amounts are estimated at more than 50,000 US dollars.

After receiving several complaints, the cybercrime unit of the central directorate of the judicial police, without hesitation, undertook digital investigations that led to the arrest of the suspect, who bluntly acknowledged the facts against him and asked for leniency from the authorities in charge of law enforcement. At the end of the investigations, the accused was referred to the Kaloum prosecutor's office, which requested the opening of a judicial investigation for the offences of fraud, blackmail, and extortion, all through a computer system and money laundering.

To date, the proceedings have resulted in a trial and the offender sentenced to five years' imprisonment and a fine of GNF 500,000,000 by the Criminal Court of Kaloum and his property confiscated in accordance with the AML/CFT and Cyber Security laws. MSD is in detention at Conakry's central prison.

Source: Guinea

Case 15: Trade (Import/Export) Contract Scam and Advance Fee Fraud

In July 2022, a Ukrainian National filed a complaint at EOCO alleged that he was scammed of $6.5M. Mr. X a Nigerian national resident in Ghana contracted to supply Mr. F a Ukrainian national with teak wood poles from Ghana in 2018. Pictures of teak poles allegedly packed in a custom bonded warehouses in addition to shipping documents were sent to the Ukrainian as evidence that the goods were about to be shipped. The Ukrainian parted with US$6.5M via wire transfer as payment for the products. The Ukrainian subsequently appointed two Ghanaian Lawyers V and K to supervise the transactions. V and K allegedly discovered that the transaction was a sham but led the Ukrainian on to make payments. Lawyer V confirmed receiving legal fees from the Ukrainian as well as GHS600,000 from Mr. X. Both Mr. X, V and K have been arrested a charged with money laundering and conspiracy to defraud and defrauding by false pretences. They are currently in EOCO custody.

Source: Ghana

Case 16: Fraud, Blackmail, Extortion and Money Laundering

In December 2022, AOK an entrepreneur residing in the Sonfonia district, in the urban commune of Ratoma/Conakry, received a phone call from a stranger who told him on the other end of the phone that he was a great soothsayer. Thus, the stranger described him and gave him precise information about his family, his activities, his privacy and then revealed to him that he would run a great danger if he did not make great sacrifices to prevent what was about to befall him. The sacrifices proposed included: 10 oxen, 2 camels, 5 sheep to be sacrificed and an amount of 25 million francs (2,500 USD) to be used to buy other items that were to be considered for occult work.

The stranger advised him not to explain this situation to anyone else, even his wife, at the risk of being affected by madness. He advised her to act quickly because time was of the essence. Astonished, upset and frightened by such unexpected statements and fearing for his life, he gathered the amount of 25 million as well as the value of the animals mentioned above, all thus making 110,000,000 FG (11,000 USD). He asked the stranger, who is none other than IKK, to indicate how he could send him this amount as soon as possible.

The suspect thus gave him 5 telephone numbers with mobile money accounts on which he asked him to split deposit of the amount, at the rate of 22,000,000 FG per account. After making the payment, the suspect asked him to fetch seawater at midnight, pour this water into a jar still unused and new, to add fresh cow milk to the water and to wash with the mixture on the following morning after observing a fasting throughout the process. He asked him to stay away for 3 weeks, after the ritual, without touching a woman.

A month after performing the ritual, AOK received another phone call from the suspect who still informing him of another dream, including his children, surrounded by a pack of black dogs that threatened to devour them and that the fate had to be quickly averted to prevent the children from being victims of witchcraft. As for the first time he indicated animals to sacrifice and an amount of 26 million (2,600 USD) to pay. Frightened by this new revelation, AOK refused to comply and claimed that he no longer has the means to face the new requirement of the soothsayer. The suspect upon hearing this started to threaten AOK other numbers and sometimes, through intermediaries.

Worried about the situation, AOK decided to inform his wife going against the warning of the so-called soothsayer. The wife informed her brother, who is a judicial police officer, who advised her brother-in-law, to immediately file a complaint with the Cybercrime Unit of the Central Directorate of the Judicial Police.

Upon receiving AOK's complaint, the Cybercrime Unit of the Central Directorate of the Judicial Police, without hesitation, immediately commenced investigations by studying the digital identification of the users of the various numbers used to exchange with him. A requisition was therefore sent to the ARPT for the purpose of communicating incoming and outgoing call histories of suspicious numbers as well as the geolocation of users. The results of the digital investigations indicated that the phone calls came from Labé, specifically from the detention centre. A mission was dispatched, under the direction of the public prosecutor, to reprimand the accused persons operating from this detention centre. After half a day of searches of the various cells, 22 phones were seized. After intense investigations, the prisoners finally collaborated and denounced their fellow prisoners involved in the scam, some of whom had already removed the chips from the phones.

When questioned by the investigators, IKK, the main perpetrator, faced with a fait accompli, acknowledged the facts of fraud and extortion through a computer system for which AOK was a victim, and denounced his accomplices who were none other than ELMO, which played the role of cattle seller, ELGA which was responsible for going to the various mobile money kiosks in order to withdraw the various amounts. He also denounced FORCE, the prison guard who not only facilitated the acquisition of mobile phones, but also served as a conduit for collecting money on behalf of the suspect outside the detention house, in return for bribes. IKK also denounced two cattle breeders and a butcher who allowed it to launder the proceeds of its cybercriminal acts.

At the end of the investigations, the defendant and his accomplices were referred to the Labé prosecutor's office, which requested the opening of a judicial investigation for the offences of fraud, blackmail, and extortion, all through a computer system and money laundering. To date, the accused have all been referred to the trial court, in the Criminal Court of Labé.

Source: Guinea

Case 17: Fraud, Impersonation, Advance Fee Fraud, and Money Laundering

The EOCO received an intelligence report from the Financial Intelligence Centre (FIC) in January 2017 that the first accused (A1), a foreign national and a holder of US passport received various remittances totalling GHS1,551,953.55 (USD309,000) into his account with a bank in Ghana. It turned out that A1 opened and operated the bank account with forged ID card and other forged documents that misrepresented that he was a UN ambassador. A1, prior to opening his bank account, had also received several remittances via MoneyGram and Western Union transfers.

When A1's funds were held, due to the suspicious nature, for further investigation, the second accused (A2), using forged documents in the name of prominent Ghanaian ministers represented himself as a lawyer for UN in Ghana, and attempted to obtain the release of the funds to A1. A2 claimed that the funds were from Singapore and were meant to be given to A1 to help pay institutions like Ministry of Finance and Bank of Ghana for some alleged UN projects being executed in Ghana. A1 alleged that he was in Ghana to undertake a project for refugees and that he had been a UN ambassador-elect for refugees since 2015. Investigations however found out that A1 was not a representative of UN and had never undertaken any project for UN. Investigations showed that those remittances were proceeds of crime, which source and purpose A1 and A2 sought to disguise.

The third accused (A3), then a branch manager of the bank where A1 opened his account deliberately violated the account opening procedures and KYC regulations to enable A1 to receive and disguise the tainted funds. The bank upon detecting the violations, filed suspicious transaction report (STR) with the FIC, which also referred the case to EOCO for investigations. The investigation had not been able to interview the remitters to confirm that the remittances were

fraudulent, and there had been no complaints of thefts or fraud lodged against the accused by the remitters. All attempts made by the investigation including the use of Mutual Legal assistance proved futile. That notwithstanding, the suspects were accordingly charged with money laundering, forgery of documents, impersonation, defrauding by false pretences, abetment of forgery, aiding and abetting money laundering, contrary to Sections 1& 2 of the then Anti-Money Laundering Act, 2008 (Act 749), disobeying an obligation contrary to the Immigration Act, 2000 (Act 573) and charges of tax evasion contrary to Section 149 of the then Internal Revenue Act, 2000 (Act 592). Prosecution is still on-going.

Source: Ghana

Case 18: Online Trading Scam, Impersonation and Advance Fee Fraud

In October 2021, Ms. ANDA from Bafata, contacted the police, on an alleged online scam perpetrated by a suspect from neighboring country. The suspect was purportedly selling artificial hair displayed on his Facebook page with the name Tafa Cabélo. The suspect will contact his victims immediately they express interest in purchasing the hair. The suspect Tafa told Ms ANDA that the hair he wanted cost 190,000 FCFA (300 USD), but she most makes an advance payment via mobile money of 50,000 FCFA (95 USD) to place an order. As Ms ANDA was interested, she sent the mobile money. Not hearing from the suspect for weeks, she called to enquire about the order, which the suspect replied that his cargo was about to arrive. After some time, the suspect called her, asking to come forward with an additional 90,000 FCFA so that he could dispatch her order to the border. The latter request arouses Ms ANDA's suspicion which she did not disclose to the suspect but alerted the Bissau border police. In agreement with the police, she created a story, which involved her brother NANO, residing in Pefine. NANO then called the suspect as agreed by Ms ANDA confirming he would be delivering the requested amount at the border. The police later guide them on how to proceed in terms of communication with the suspect, as they executed the arrest of the suspect next to the ELTON fuel station located in Bandim.

Furthermore, an analysis of the suspect phone revealed that he has been deceiving women for a long time with allegedly selling hair, through his Facebook account and consequently in Messenger and, for this purpose, he created two accounts on the partner networks with the following names: FALL TÈRANGA EL TIFRÈ and TAFA CABÉLO, in order to lure his victims.

The suspect was handed to the Public Prosecutor's Office for further investigation and prosecution.

Source: Guinea Bissau

Case 19: Trade (Import/Export) Contract Scam and Advance Fee Fraud

In 2019, the agency responsible for fighting cybercrime received complaints about certain individuals engaged in an export contract scam case. This organized gang from within and neighbouring country through telephone contacted the victim GSS pretending to have met and known him long ago. After convincing GSS that they are old acquaintances and purporting to be medical doctors, proposed some export deal that has to do with the supply of "Artemisia" root. They then persuaded GSS on the need to make transfers to meet the export costs (purchase of the product, storage, transport, packaging, customs formalities and others), and manage to fraudulently extort money from him. GSS transferred the funds which were withdrawn via electronic means (Mobile money, Western Union, etc.). The investigation led to the arrest of SKS and 47 other suspects, including a national from neighbouring country, identified as an active member of the gang.

The matter was referred to the Special Prosecutor at CRIET and after finding the accused guilty, the court sentenced SKS to seven (7) years imprisonment with one million FCFA (1,522 USD) fines and ordered the reimbursement of one million seven hundred and thirty-six thousand one hundred FCFA (2,642 USD) to GSS.

Source: Benin

Case 20: Romance Scam / False Pretence and Advance Fee Fraud

In 2019, the lead agency responsible for fighting cybercrime received an intelligence about an organized cybercrime gang residing in Cocotomey in the Gbodjè district. Upon investigation and uncovering the location of the gang members, LCD, KRH and DR were arrested in January 2020. LCD disclosed using the profile of a woman to lure his victims into romance scam, while KRH uses on his profile the photo of a needy woman seeking financial assistance. As for DR, he offers on the internet fictitious contracts to secure loan. KE an accomplice was responsible for making withdrawals of funds generated from these cybercriminal activities was also arrested. The case was referred to the Special Prosecutor at CRIET, they were tried and the Court upheld the offense of complicity in the account of KE and the offense of fraud by means of a computer system or an electronic communication network by sentencing LCD, KRH and DR to five (5) years of imprisonment each and a fine of two million FCFA (3,044 USD).

Source: Benin

Typology 5: Ponzi Scheme Fraud and Money Laundering

39. The typology presented here is one that requires the most and urgent attention considering the volume and value of funds involved from the cases submitted. The typology is either related to virtual asset / cryptocurrency or online investment. A combination of greed and limited knowledge of the proposed business venture entered are the motivating factors for most of the vulnerable victims that have fallen prey for the schemes used by these criminals. Also, the modus operandi used here where possible because of the inadequate regulatory and enforcement framework in member States.

Case 1: Virtual Asset Ponzi Scheme Fraud

Company "A" was incorporated in Accra in October 2017 with the following objects which include real estate development, transportation services, ecommerce, e-trading, blockchain technology services, mobile money transfers, road construction, import of solar energy appliances, oil and gas services. Soon after incorporation the company falsely represented to the Ghanaian public that they were licensed to carry on deposit taking business by Bank of Ghana when in fact they were not authorised to do so. The Scammers promised victims a monthly return of 27-percent on the investment. The company succeeded in receiving GHS43.2M (approximately USD9.6M) from unsuspecting persons. The amount received was dissipated leaving a balance of GHS3.7M (USD820K) which was frozen by the court. The accused persons during investigation admitted that their company was not licensed by Bank of Ghana and Securities and Exchange Commission (SEC) to engage in any such business. They also claimed that they were commercially trading in cryptocurrency online which had crushed. This claim could not be explored further for repudiation or confirmation by the investigation because the investigators did not have the requisite technical acumen to ascertain the veracity of the claims being made by the accused. Investigation however established that the company was just using the cryptocurrency trade as a cover to obtain deposit from the public. As a result, the accused were charged and are being prosecuted for operating a deposit taking business without license, defrauding by false pretences and tax evasion. No charges in relation to the illegal trading of Bitcoin was proffered because the investigation did not have the technical acumen to explore whether the accused was involved in the business of cryptocurrency, and the destination of the funds. The Economic and Organised Crime Office (EOCO) initiated the investigation based on petitions and complaints received from some of the victims of the fraudulent scheme.

Source: Ghana

Case 2: Virtual Asset Ponzi Scheme Fraud

In February 2020, the suspect entered the country by road using unauthorised route and was in possession of 10,000 USD, which he did not declared as mandated by law and regulation. The suspect registered a Sole Proprietorship Company in Bissau called CHAVE DE SUCESSO, with the Center for Company Formalization of the Ministry of Economy. Empresa Chave do Sucesso started its financial operations in March 2020, receiving deposits from individuals attracting 20% interest weekly. The suspect created a register and trained his marketing staff who mobilize clients to invest their money in the company with the possibility of earning 20% profit weekly.

The marketers were earning 60,000 FCFA (100 USD) for their service and an additional commission of 3% on the amount deposited by each customer they bring to the company. To convince his victims, the suspect presented his Bank Account details domiciled in a bank in the capital Bissau, in which he purported to have been making transfers to purchase virtual currency. He informed his victims of his company having an account on the binimo.com platform which due to poor internet facility in Bissau has not been active on the platform.

Although the suspect company is registered business in Bissau, the company was not registered or licenced to engage in deposit taking. Investigation revealed that the suspect initially paid 5.7 million FCFA (95,000 USD) from the 70.8 million deposit he received in the month of May 2020. As at July 2020, the suspect had paid 3174 investors the money with the respective interest in the amount of 917,471,400 FCFA (1.53 million USD) and was still owing 1409 investors the sum of 532,249,200 FCFA (900,000 USD), including accumulated interest of 20% amounting to 443,341,000 FCFA (740,000 USD).

The suspect was detained by the Judiciary Police and apprehended at his company 85,361,500 FCFA (142,000 USD). He was charged with fraud, including tax fraud and money laundering. He was condemned to a jail term of 10 years and to refund his victims with the sum of 532,249,200 FCFA (900,000 USD). In addition to the refund, he is to compensate his victims with the sum of 75,000,000 FCFA (125,000USD).

Source: Guinea Bissau

Case 3: Virtual Asset Ponzi Scheme Fraud

A young man with a bit of ICT knowledge hatched up a plan to operate a Ponzi scheme. He brazenly put out adverts and jingles on social media and community radios in rural areas saying that he is operating a cryptocurrency business. His jingles and adverts promised 22% interest on capital for 2 weeks and 44% every month. In less than two months he accumulated about Le5 Billion (USD$294,724.65).

The FIU used its administrative powers and restricted the funds. The Bank of Sierra Leone was immediately notified, and an Intelligence Report sent to the Director of Crime Services, Sierra Leone Police. Among the depositors into this scheme were local politicians, police officers, teachers, rural farmers, students etc.

Investigations revealed that he had cryptocurrency wallet which had only $800. Investigations further revealed that he was not engaged in cryptocurrency business but a Ponzi scheme. The High Court is seized of this matter.

Source: Sierra Leone

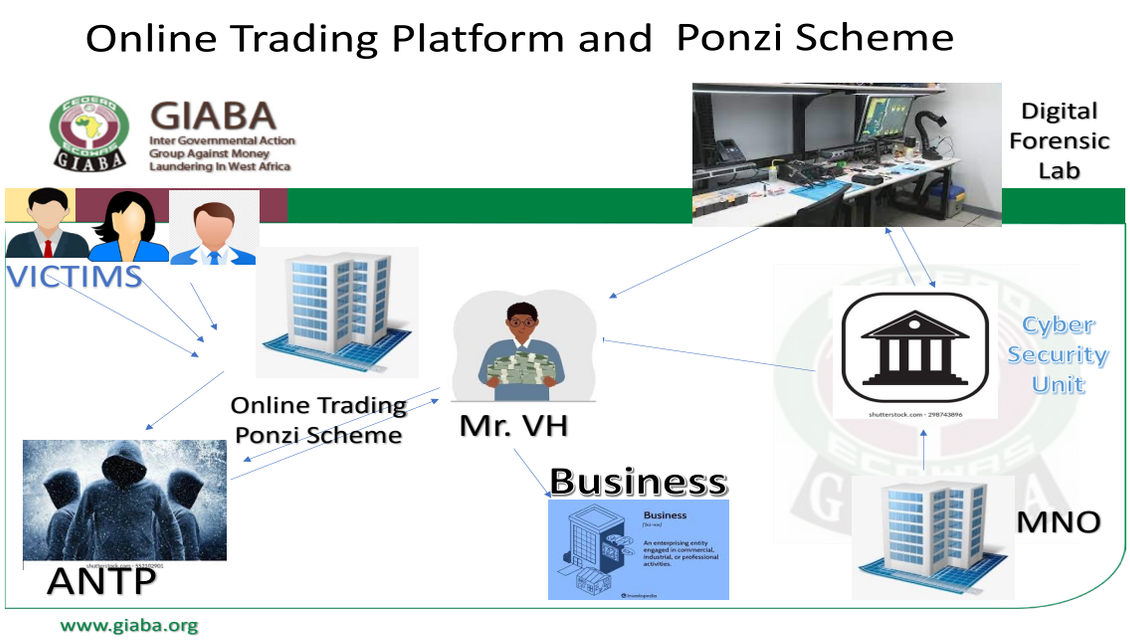
Case 4: Online Ponzi Scheme Fraud

VH is a young businessman was in the habit of making frequent withdrawals using mobile money service. He makes large sums withdrawals daily from various mobile money points. To carry out his transactions, he has several sim cards. Once one of the sim cards has reached its authorized withdrawal limit, he replaced it with a new one to continue the operations. These frequent activities aroused the suspicion of the operator, which initially thought that there was a malfunction in its platform. In order to confirm it suspicion, the operator filed a complaint to the lead agency

responsible for fighting cybercrime (PLCC). PLCC supported by the Digital Forensics Laboratory, started investigations that led to the arrest of VH. When brought to the premises and upon interrogation, he said he belonged to a network and had been recruited to make withdrawals with sim cards that were made available to him. The funds withdrawn, he said, came from an online stock market investment site called ANTP whose link is: https://www.antp.io. This site invites individuals to invest an amount of their choice for a higher return on investment. The money invested was to grow according to the number of daily tasks to be done on the site. The members had no idea of the deception. Indeed, they noticed the increase of their balance on the platform as promised. However, a few days later they were blocked and hardly received their dues. Except for a few who received money on their mobile trading accounts in order to push them to invest more and attract the maximum number of people. As a result of the search and seizure, the PLCC arrested 12 members of the network. They are ZQ, XC, KY, MK, TBF, SL, SAM, MT, ME, MA, KKY, MM. They had in their possession hundreds of phones, 08 laptops and the sum of 46,553,000 CFA francs (75,000 USD).

The provisional loss was estimated at more than 1,000,000,000 CFA francs (1.6 million USD). Several transactions were carried out and the funds deposited on a bitcoin account to bypass the mechanisms. (The case is still ongoing at the time of reporting

Source: Cote d'Ivoire



Methods and techniques

- Creating Ponzi scheme website with features of online trading and investment platform.
- Enable website Pop up on potential victims' social media page.
- Making part payment to initial victims/investors to lure them invest more and have others trust the process.
- Fictitious increase in the Return on Income (ROI) of victims/investors to lure them to invest more.

Red flags & Indicators

- Non F2F investment opportunities with online start-ups.
- Unrealistic business offer – Super profit due to very high ROI.

Case 5: Mobile Money Investment Ponzi Scheme Fraud

In 2022, a case of fake investment was reported to the Fraud Squad of the Gambia Police Force by 146 victims. A so call investment call Qubid was introduced in the Gambia by a fictitious name Marcus Gabel who is believed to be in Nigeria. He recruited agents in the Gambia to carry out the supposed business form the nature of the business is the agent encouraged people to invest with them through mobile money and bank deposit and receive their capital and 20% interest after seven days.

The first group of people who invested received their various capital interests which encourage many people to invest in the business. A total amount of D24,526,993 (USD 437,982) was invested in the business by 146 people part of the invested money was used to pay for capital and interest of investors whose investment were matured. That one of the agent sent an amount of D2, 834,000 (USD 50,607) worth of Bitcoins and D551,125 (9,841) to Marcus was in Nigeria. This money was meant to be the investment funds.

Investigation revealed that the said company was never registered in the Gambia and the one who initiated the business was in Nigeria and he was managing/controlling the business through a WhatsApp group. The 4 agents were charged with money laundering, obtaining money by false pretence and carry out banking business in the Gambia without license and currently standing trials at the Gambia High court.

Source: The Gambia

Case 6: E-Commerce Investment Fraud

During 2019, the Central Brigade for the Fight against Cybercrime (BCLCC) received several victims who wanted to file a complaint against the company Chymall for fraud and breach of trust having caused damage of more than one billion CFA francs.

From the hearing of the head of the company, it appears that the company has joined an online trading platform called SAIRUI. With the evolution of their activity, they were promoted to a center on payment of a sum of ten thousand (10,000) dollars. Their position as a center made them intermediaries through which other people could join this platform, receive the products and their possible bonuses. In June 2020, following the change of name of the company which became Chymall, a representation was created in Burkina Faso. They then began to register other people who wish to join the platform, under the sponsorship of the leaders. Things went normal for awhile and people who accessed the platform through their center started to receive their bonuses in accordance with the rates set by Chymall. However, in November 2020, they started facing payment challenges and anomalies which did not comply with the pre-established rules. Also, all accounts on the platform have undergone a change.

Further investigation revealed that the parent company was based in China with representation in Ghana. To date, we have more than one thousand (1000) victims with damages amounting to more than one billion CFA francs (1.6 million USD) unaccounted for.

Source: Burkina Faso

Case 7: Online / Non-Face-to-Face Loan Scheme Fraud

Mr. AS engages in cybercrime by posting online loan messages under false identities in order to defraud his victims. The investigation led to the arrest of AS, residing in Abomey-calavi, in the Bidossessi district, in September 2019. Following his arrest, AS was found with false documents relating to loan contracts, transfer orders, insurance guarantee certificates, money transfer copies found in his telephone and laptop in his possession. He alluded having used the funds he extorted from victims to pay for a vehicle, open a clothing store, and make other investments. He directed his victims to pay advances of the costs of securing the loans to the bank accounts belonging to his accomplices who

in turn make withdrawals. The case was referred to the Special Prosecutor at CRIET in September 2022. AS was tried and sentenced to five (5) years imprisonment and a fine of five hundred (761 USD). All the asset related to the case were confiscated.

Source: Benin

Typology 6: Mobile Money Related Fraud and Money Laundering

40. The second most popular typology after advance fee fraud in West Africa, is mobile money related fraud. There is thin line between advance fee fraud and mobile money related fraud. In fact, almost all advance fee fraud is enabled by mobile telephone and in most of the small and medium payment uses mobile money platform to receive advance fees demanded or requested. Some of the cases presented under advance fee fraud may equally be suited to be presented as mobile money related fraud.

Case 1: False Pretense, Impersonation, Forgery and Mobile Money Fraud

A branch of a bank's customer service line received a call purportedly from the bank's Head Office. The caller identified himself as an executive committee member (EXCO Member) by using the name of Chief Operating Officer (COO). After a brief telephone conversation with the Customer Service Officer, he requested to speak to the teller who handles Mobile Money operation at the branch. The call was transferred to the teller where he indicated to the teller that he wanted to take the teller through how to conduct mobile money reversals on the Momo platform. He then requested the teller to enter her MoMo PIN and upon entering the PIN the suspect gave series of instructions which the teller obliged. Immediately after the suspect got off the phone, the teller noticed that a total amount of GHS37,000 (USD6,491) was fraudulently transferred from the Bank's wallet to an individual's wallet which was immediately withdrawn.

The case was reported to the police who with the assistance with MTN Ghana tracked the suspect, a 30yr old man to his hideout in a distance remote town and was arrested in March 2021. During investigation, it was established the ID card used by the suspect to register his SIM card was forged. The suspect has been charged for forgery, impersonation, defrauding by false pretences and money laundering. Prosecution is still on-going at the circuit court.

Source: Ghana

Case 2: False Pretence, Impersonation, Forgery and Mobile Money Fraud

A suspect Mr. ABD was arrested in July 2021, on suspicion of alleged scam through social media. The suspect along with other accomplice was using Facebook and Messenger under a false profile name (SOIOIO MELA) and cunningly deceiving his victims, extorting money from them. In addition to Facebook messenger, he also uses mobile phone numbers registered in other people names to communicate with his victims. Preliminary investigations led the police to two individuals who had visual contact with the suspect, as he had asked them to use their mobile phone numbers, to receive money transferred to him. These individuals confirmed that they would recognize him if they met him. The investigation reconciled the above information with the disclosure made by Mr. BILL, commonly known as SOIOIO, when he accompanied one of the victims to present the complaint to the Police. Mr. BILL confirmed to the investigation suspect is an individual commonly known as SACA, who, in collusion with his niece named SC, had used his cell phone, which the his niece had stolen from her residence in Bula, with which they had committed similar acts and putting his reputation in question, as they were asking for money in his name, as well as sending love messages to his friends and acquaintance?, bringing into disrepute the matrimonial relationship of some of the people they targeted. He was, however, able to recover his cell phone with the intervention of the Judiciary Police.

The suspect was under the custody of the Public Prosecutor's Office, ready to be tried at the Crime Branch of the Regional Court of Bissau, while waiting for expert examination of the cell phone (Infinix Smart Dual Camera) seized from him.

Source: Guinea Bissau

Case 3: False Pretense, Impersonation and Mobile Money Agent Fraud

In February 2018, a District Magistrate Court at Oda in the Eastern Region of Ghana jailed two persons aged 28 and 29 respectively for defrauding a mobile money agent. According to the Police, the suspects called the mobile money on phone and pretended that they were officers from MTN Ghana Ltd calling to educate the agent on his mobile money transaction. However, during the process, the mobile money agent noted that his account was debited with GHS2000. The agent reported the incident to the police who liaised with MTN and had the suspects tracked and arrested. One of the suspects claimed to be an expert in Information and Communication Technology (ICT) and the other unemployed. The two suspects were prosecuted and jailed.

Source: Ghana

Case 4: Insider Dealings, Hacking Using Complex Engineering Scheme and Mobile Money Fraud

Bank X in Ghana had filed a petition with EOCO for unauthorised withdrawals made from a number of their customers' accounts via the bank's mobile banking and internet banking platforms. The fraudulent withdrawals were made when the customers were in the process of getting on-boarded onto the electronic banking. Prior to bank X's petition, two other banks, Y and Z, had also made similar complaints about unauthorised withdrawals from some of their customers via Mobile Banking application and four suspects were arrested by EOCO. Investigation noted that the attackers were running complex social engineering schemes targeted at unsuspecting persons to obtain relevant log-in credentials to the electronic banking portals. Some of the suspects had obtained customer details (including account number, account name, account balance, date of birth, address and phone numbers) from co-conspirators from some of the banks. Armed with this information, they called the customers with cloned numbers which appear as though the calls emanated from the banks and tricked the victims into giving out their details. Once these credentials were obtained, funds were layered and laundered through an elaborate scheme comprising the use of multiple mobile money accounts and third-party agent bank accounts. In some instances, few moments after the unauthorised withdrawals, the funds were immediately withdrawn from Mobile Money Merchants. Investigation is still on-going.

Source : Ghana

Case 5: Insider Dealings, Impersonation and Mobile Money Fraud

In April 2022, EOCO arrested a bank official and a staff of a leading telecommunications network who reportedly connived with some four persons to defraud some bank customers via SIM swap fraud. The suspects engaged the bank official to provide them with bank account details and phone numbers of their victims with huge account balances to assist them withdraw funds from their accounts, while the telco staff was contacted to clone the phone numbers of the victims for the operation. The bank staff connived with the accused persons by providing the requested details and they were able to clone phone numbers of some three customers with the intention of stealing GH¢850,000; GH¢680,000 and GH¢50,000 (a total of USD216,000) respectively from the customers. The accused persons set up a mobile application with the cloned SIMs to withdraw the funds from the customers' bank accounts. Meanwhile, the bank official had notified the Bank about the plot and the issue was reported to EOCO. The accused persons were arrested as they sought to withdraw the funds from the Bank. They have been charged with nine counts of conspiracy to steal, attempt to steal, and participating in an organised criminal group. The case is being prosecuted.

Source: Ghana

Case 6: Impersonation, Mobile Money and Sim Card Fraud

Mr O, a young graduate started his own enterprise, selling sim card, in order to acquire financial independence. His business was doing well before one faithful day when approached by KDU who requested to buy 5 Sim cards. The idea is to use them to open five mobile transfer agencies. Mr O activated the sim cards and as usual the customer was satisfied. As he continues his business, Mr O learned that the Sim cards he sold to KDU were used in fraudulent transactions. He was surprised because KDU had told him that the cards were for the five cashiers in the branches he was about to open. KDU had provided Mr O with five different IDs for the activation of the sim cards. He was worried because he also heard rumours that the e-wallet scam was going around. Moreover, he was summoned weeks later by the cybercrime police for a similar case. Indeed, the Platform for the Fight Against Cybercrime (PLCC) is currently overwhelmed by complaints related to this offense. Among them, those of three victims LLF, CNS and MYL who claim to have been contacted by unknown persons by phone. They claimed to have made deposits by mistake on their numbers. To verify the effectiveness of the alleged transactions, the victims emptied their wallets to an unknown number. Each of them filed a complaint with the PLCC to solve the case.

The PLCC's investigation, supported technically by the LCN (Digital Forensics Laboratory), led to the discovery that the number receiving the transfers belonged to KDU. The suspect was arrested and was in possession of 27 Sim cards. During his interrogation, KDU admitted to having scammed several people on their mobile accounts with the chips purchased from Mr O. The LCN's analysis of the 27 sim cards also revealed that they were used for other fraudulent transactions. These numbers were the subject of 136 complaints and made 308 fraudulent deposits amounting to 12,786,202 CFA francs (19,520 Euros).

Ultimately KDU was brought before the Abidjan Public Prosecutor's Office where he could be prosecuted for fraud and complicity in transaction fraud. (The case is still ongoing at the time of reporting)

Source: Cote d'Ivoire

Case 7: Insider Dealings and Mobile Money Agent Fraud

In January 2022, the Central Brigade Fighting Cybercrime was contacted by the manager of the C2EGF-BF company who filed a complaint against one of their sale representatives for forgery and use of forged documents, breach of trust and money laundering having caused a loss of more than thirty-seven million CFA francs (60,000 USD).

From the investigation, it appears that the respondent had been recruited by the C2EGF-BF company as a sale representative. The company is a Mobile Money distributor. The accused job was to recruit, train and assist points of sale agents for company. The latter took advantage of his commercial position to install a lady and this lady called at the level of the company to ask for supplies. Receipts justifying reimbursements went through the latter.

Further investigation led to the arrest of the suspect. Once the shop asked for a supply, for refunds, the latter had old receipts that he had scanned. He would take an old receipt, changed the date, take a photo and send it to the company via WhatsApp as an instant message. As soon as the message is read, it is deleted immediately. The respondent used the money from his package to create several other orange money shops in the name of his parents and his girlfriends. (The case is still ongoing at the time of reporting)

Source: Burkina Faso

Case 8: Sim Card Fraud and Identity Theft Using Pre-Activated Sim from Abandoned Voters' Records

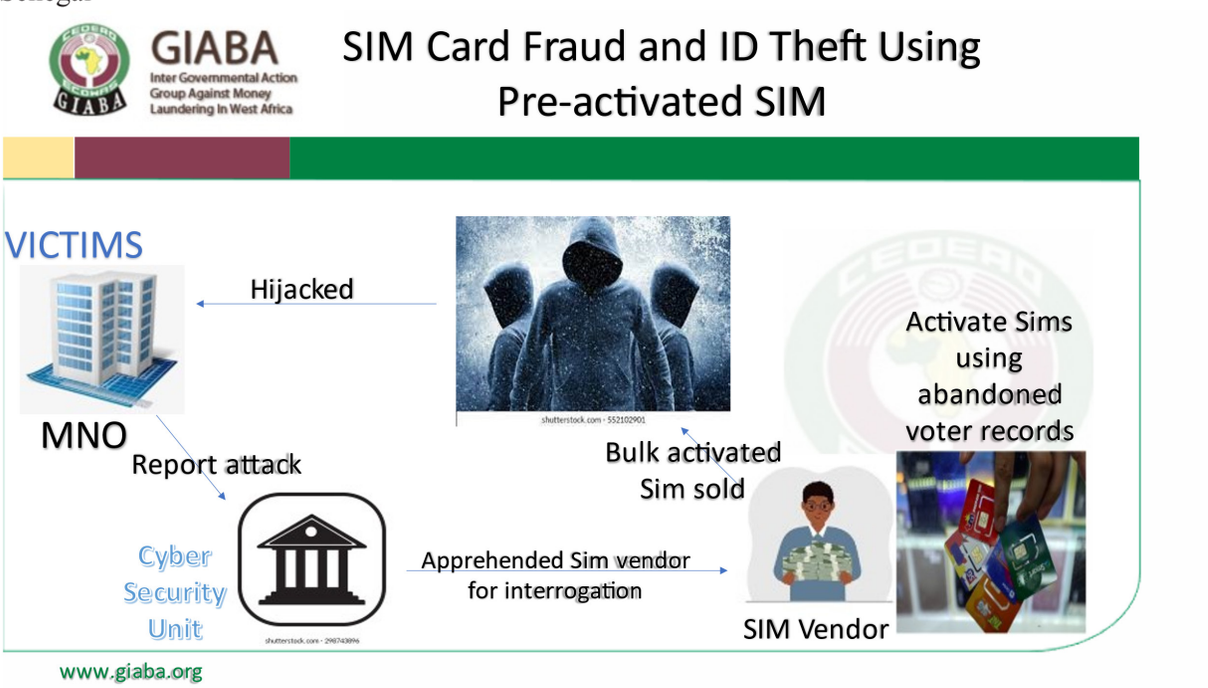
The computer network system of a company was hacked. The hacker exploited security flaws at the company's network and applications to extract money from the e-currency system. In fact, a test chip for new services was set up in a department without measures to follow up in case of an incident to determine the responsibilities.

The chip was used to position money on more than 100 e-currency accounts. The tracking of the money is made difficult by the fact that the identification and sale of the chips are not very well supervised. Thus, the money from this attack is withdrawn from various stores in several cities, notably Dakar and Thiès. The details of the operations suggest the use of a means of transport to withdraw the money from all the stores on the Dakar-Thies axis.

An investigation was launched following a complaint from the company that was attacked. It was noted that different chips had been activated beforehand without being able to establish the identity of the true owners. These same chips were later used to open electronic currency accounts.

Investigations within the structure have not been able to determine the origin of the connection that carried out these fraudulent operations. Moreover, no system of validation of operations or watch for important operations was established. The investigation was thus directed on the track of the chips in order to establish the identity of the true owners in order to identify the final recipient of its operations. Thus, the seller who proceeded to the activation of the different chips was interrogated. Being unable to provide the identity of the purchasers, a search was carried out at his home. It was thus discovered that he himself had proceeded to the activation of the different chips on the basis of the personal data contained in the electoral file. In fact, after each election, the files are recovered and sold on the market. This constitutes a major flaw in the application of the measure requiring telephone operators to identify their customers.

Source: Senegal



Methods and techniques

- Use of fake identities to impersonate individuals/entities
- Scammers impersonate customer service agents and ask users to share PINs, OTPs (One-Time Passwords), or account details purporting to be assisting the customer "fix an issue."
- Use of mobile phone numbers registered in other people's names
- Use of complex social engineering schemes to obtain log-in credentials to the electronic platform of individuals/entities

Red flags & Indicators

- A mobile money account suddenly receives or sends large sums of money, inconsistent with previous activity
- Multiple high-value transactions within a short period
- Funds are immediately withdrawn or transferred to multiple accounts within minutes of receipt
- Series of funds transfers from a wallet or account into multiple accounts or wallets at short intervals

Typology 7: Cyber Enabled Terrorist Financing Cases

41. As terrorist financing is still a complex phenomenon that the region is still grappling with, particularly understanding the modus operandi which are largely believed to be occurring in the informal sector and perhaps using the cyberspace, including the dark web, there are 3 cases submitted that qualifies as cyber enabled TF cases.

Case 1: Trade Based Terrorist Financing

A Canadian citizen of Somali origin residing in Dakar had created a real estate company in Senegal. The company, in conjunction with a Senegalese, had opened an account with a bank in Dakar. Sometime later, the account received a transfer of approximately one hundred and six thousand (106,000) US dollars from a Somali national residing in the United States. The transfer was executed by a financial institution based in Dubai. Suspecting this operation, due to the poorly documented identity of the new client and the destination of the funds, the Senegalese bank filed a suspicious transaction report with the FIU. The investigation revealed that the company had no legal status in Senegal and that it had been created specifically for the purpose of laundering illicit funds through the sale of imported goods. In addition, the individuals involved were in contact with extremist groups involved in terrorist activities in East Africa, America, and West Africa. Other companies were created, in association with Senegalese, to import used goods, some of which were sold in Dakar and the rest exported to another country for resale. The proceeds of these various commercial operations were subsequently sent to several terrorist groups through various channels. (The case is still ongoing at the time of reporting)

Source: Senegal

Case 2: Suspected Fund Raising for Terrorist Financing

In 2015 XPTO Bank filed an STR relating to an individual identified by XMAN, a Turkish by nationality, residing in Praia, and a self-employed teacher. His financial transactions include making withdrawals and foreign exchange transfers abroad, he also receives funds specifically from Turkey. It was found that payments were offset by the visa holder in amounts equal to the credits deposited in cash on the same day or the following day. Operation of purchases of foreign currency for a considerably high amount without justification, considering the customer is a self-employed teacher as he declared to the XPTO Bank.

Account movement characterized by many small credit amounts and a small number of high value debits. Justification XMAN gave for the intended purpose of the funds being for religious purposes, does not tie with the actual payments made for communication services, accommodation, and frequent travel. Absence of any reasonable relationship between XMAN and the PPP company, whose purpose is the sale of computer equipment.

After analysing the STR from the XPTO Bank, it was found that Mr. XMAN holds two separate accounts (national and foreign currencies), at the bank in question, opened in in September and December 2012, respectively. For the account opened in December 2012, he received transfers from the Turkish bank KATILIM BAKAST A. S., in a total amount of 5,669,379$00 CV Escudos (51,416 euros), in (04) four movements with reasons for the transfers being to make payment for Qurban (animal sacrifice) and to orphanage organisations. The amounts received through the transfers indicated above, between January and May 2014, were used by Mr. XMAN to make payments with XPTO bank checks for sustenance and travel, and not for religious and charitable purposes as stated in the transfers. Payments were made to Company PPP that sells equipment and QQQ that imports various food products, as well as payment to a travel agency.

Between 2013 and 2014, Mr. XMAN made several trips, including 9 (nine) between PRAIA/DAKAR, 4 (four) between PRAIA/MOROCCO, 5 (five) between PRAIA/PORTUGAL and 1 (one) PRAIA/BISSAU. The case in question is still under investigation.

Source: Cabo Verde

Case 3: Terrorist Financing through Informal Transfers Methods (HAWALA)

In 2022, the State security services made available to the investigation services Mr. DA, a motorcycle carrier and trafficker, suspected of being a collaborator of an armed terrorist group led by Mr. IL. IL is a wanted criminal, cited in several cases of extortion, looting, and serious violence against civilians in Niger, including his involvement in terrorist activities in Liptako Gourma. IL, according to information sources, leads an Armed Group using acts that qualify as terrorists under the Nigerien legislation.

From the investigation, IL has been using false name, with false ID, an unidentified phone number, to sends money frequently from his location to some destination in DOUT, a border town in the south of the country, a relatively secured area where many traffickers of all kinds are located. He has been transferring funds to DA using Hawala. Once the transfer is done, DA receives an alert message on his phone indicating the deposit of funds made in his name. He also receives a phone call from IL confirming the amount of money sent. DA withdrew the funds, then later went to the border town close to DOUT to buy motorcycles deliver it to the area where IL operate.

In addition to the funds (500,000 FCFA / motorcycle) intended for the purchase of motorcycles, DA receives an extra 50,000 to 60,000 FCFA (100 USD) per motorcycle conveyed to the North-West border of Niger.

Source: Niger

CHAPTER 4

RED FLAGS AND INDICATORS

42. This chapter flowing from the previous presents the red flags and indicators observed from the cases presented. Red flags and indicators are activities or actions that underpins certain activities, actions, transactions, or events, with some anomalies that raise suspicion and/or inconsistencies when subjected to rational scrutiny. These anomalies or inconsistencies leading to the suspicion requires further examination, interrogation, investigation or at least, monitoring by reporting entities, supervisors, and the public. There are a number of indicators and possible red flags that were identified from the analysis of the cases presented in the previous chapter. The indicators and red flags differ depending on the extent of the money laundering or terrorist financing activities. While the indicators represent events that may or may not indicate the existence of money laundering or terrorist financing, red flags represent events that provide strong or clearer evidence of money laundering or terrorist financing.

43. Below is the list of indicators and red flags that were identified from the analysis of the full cases, though not exhaustive. The indicators and red flags confirm that informalities, lack of awareness of cyber threats by the public, inadequate resources invested into cyber security by businesses and public institutions / organizations, weak architecture, and regulatory systems and monitoring of the cyber landscape in the region, and weak enforcement systems has a spiral effect on cyber and cyber enabled crime, money laundering and terrorist financing in West Africa.

Indicators

- Corporate client with an established relationship changes the payee account details (e.g., IBAN code) for a known beneficiary.
- There is a mismatch between the name of the payee in the payment instructions and in the account details (e.g., IBAN code).
- Use of informal remittance services (such as the 'Hawala' type of services) for cross-border transfers.
- Mismatch between the economic activity, and fund in question, either for remittances purposes or bank transaction.
- Differences in spelling of the beneficiary's name from what is on the identification documents produced for withdrawals.
- Use of money or value transfer services or remittance providers to receive funds from unrelated customers.
- Use of mules (front men), straw accounts, couriers, etc., in moving funds.
- The beneficiary's account may belong to an offshore company or be held by a financial institution located in a high-risk jurisdiction, as determined by the financial institution and relevant competent authorities.
- Purported package from an online friend that attract paying certain amount before receiving it.
- Being instructed to invest through mobile money in a suspicious company that is not registered or have office structure in the country.
- Client requesting a transaction (payment) to be carried out urgently or requests that it should be treated as confidential.
- Instructions for payment are received from a new employee of the corporate client.
- Unusual and high value transactions being ordered solely by way of email

- Change requests for a payee Bank Account made shortly after an initial order (especially if made by email)
- The corporate client with an established relationship requests a payment to be made to a suspicious "first time" beneficiary.
- The transaction is related to buying or selling the virtual currency (e.g., Bitcoins, Litecoin, Ethereum, Zcash) or similar virtual assets.
- The client requests a transaction to be carried out urgently or that it should be treated as confidential, especially if just before closing hours, weekends or public holidays.
- Cash withdrawals, or transactions disbursing a received amount, made shortly after a deposit of of an amount that is received from abroad, or under unclear, unusual title.
- The client ordering a payment to be made to a beneficiary only communicates with the beneficiary via e-mail
- Transaction which results in significant, but inexplicable, activity on the account which was previously mostly dormant/had low account turnover

Red Flags

- Regular remittances from multiple senders to the same recipient or related persons, including remittances from one or more senders in different countries to a local recipient. Particularly, when recipient do not have any relationship with senders.
- Remittances over a short period of time and structured just below the reporting threshold that together represent a large sum of money.
- Sudden inflow of funds in cash followed by sudden outflow through financial instruments such as checks.
- A financial institution receives a wire transfer for credit into an account; however, the wire transfer names a beneficiary that is not the account holder on record. This may reflect instances where a victim unwittingly sends wire transfers to a new account number provided by a criminal impersonating a known beneficiary, supplier or vendor.
- Uses of remittance services for the payment of goods and services ordered online.
- Message sent under the guise of a telco promotion and the recipient is asked to input their PIN as a verification measure to claim their "prize."
- Receiving a SMS that indicates a deposit into a customer's account, subsequently receiving calls that the deposit was a mistake and to send that amount back.
- Receiving call from a delivery company under the pretext of delivering goods from friends/relatives abroad. You are then instructed to make a deposit to a mobile money account for delivery service.
- Attractive and too-good-to-be-true business proposal from a purported acquaintance who wants you to replace a supplier of local products that is in high demand abroad.
- Request to participate or invest in businesses that attract super normal returns

- Receiving an email with a link suggesting that either your account has been hacked, or your nude photos are on the internet, or your loved one needs immediate health care, or some other kind of blackmail / cyber-attack is about to happen and you must follow certain instructions, including clicking the link sent to you.

- An unusual request from a friend / relative asking for emergency financial assistance and you should communicate only by messages.

- Messages relating to admission, or job recruitment, or winning a prize from online game for which you did not participate, can be a phishing attack or even recruitment to a terrorist group.

- Requests received asking someone to update their personal data associated with banking information and the like.

- A mobile money account suddenly receives or sends large sums of money, inconsistent with previous activity

- Funds are immediately withdrawn or transferred to multiple accounts within minutes of receipt

- Series of funds transfers from a wallet or account into multiple accounts or wallets at short intervals

CHAPTER 5

LEGAL, REGULATORY, SUPERVISORY AND ENFORCEMENT FRAMEWORK AND THEIR ASSOCIATED CHALLENGES

44. West Africa, in recent years, has witnessed a tremendous surge in its cyber space and the use of the space, leading to growth in businesses, profitability, and efficiency in program implementation and delivery. The region has also, suffered from an exponential increase in cyber criminality, particularly, cyber enabled crimes. However, the rate of detection and prevention by law enforcement is very much basic. This chapter attempts to examine the legal, regulatory, and supervisory framework and the underlying challenges in enforcement and control measures in West African economies. Also, highlighted is the countries' status of implementing existing international instruments on cybercrime in line with the FATF Standards under Recommendation 36 which encouraged countries to ratify other relevant international conventions.

Legal, Regulatory and Enforcement Framework for Cybersecurity / Cybercrime in West Africa

45. There are significant legislative gaps in some countries, particularly around the powers of the central authority in charge of the fight against cybercrime and around the legal and enforcement frameworks of countries to effectively detect, prove and curb ML or TF associated with cybercrime. While the legal and enforcement framework make provisions for law enforcement action to investigate and prosecute cyber criminals, the regulatory framework in most of West Africa either has insufficient preventive measures or is weak overall. Although few countries have made some gains on obtaining electronic and digital evidence during investigation. This continue to be a challenge in some jurisdictions.

46. Also available and may be useful to competent authorities is how existing criminal legislation and the FATF Standards (which are technology neutral) are applicable in the space of cybercrime. This includes recognising how existing categories of offences (under R.3) are applicable, as well as the existing preventive measures/regulatory framework for FIs, DNFBPs and VASPs. For example, in many of the case studies in Chapter 3, it is very clear that existing categories of offences, such as fraud, theft, extortion, forgery, sexual exploitation etc., are applicable in cases of cybercrime.

47. The recognition of applicability of existing tools and Standards is important, which shows that competent authorities can act where applicable, while waiting for the enactment of new laws and regulations. This recognition is also important to incentivize cross-border collaboration, particularly under frameworks with dual criminality.

48. The table below gives the relevant cyber security / cybercrime, data protection and related AML/CFT laws, regulations, directives and guidance as provided by experts from the member States.

Table 3.1: Cybersecurity / Cybercrime, Laws, Regulations, and Directives in West Africa

Member States	Laws and Regulatory Provisions	Comments
Benin	Law No. 2017-20 of April 20, 2018, on the Digital Code; Law No. 2018-16 of December 28, 2018, on the Penal Code in Benin in its articles 161 on acts of terrorism, 162-3 relating to computers, 670 to 689 relating to cybernetic, computer offenses; Law No. 2012-15 of March 18, 2013 on the Code of Criminal Procedure; Law No. 2011-20 of October 12, 2011 on the fight against corruption and other related offenses;	Benin has a Digital Code that punishes cybercrime and the consequences it could lead to when their perpetrators use or not methods to conceal the criminal source of their income. The Penal Code in all its provisions provides for the penalties provided for punishing money laundering and terrorist financing offenses related to cybercrime. The law on the fight against corruption and other related offenses sanctions capital financing offenses, terrorist financing related to cybercrime.
Burkina Faso	Law No. 001-2021/AN of March 30 2021 on the protection of individuals with regard to the processing of personal data; Law No. 040-2019/AN of May 29 2019 on the code of criminal procedure; Law No. 005-2017/AN of January 19, 2017 on the creation, organization and operation of judicial centers specialized in the repression of economic and financial offenses and organized crime; Law No. 016-2016/AN of May 3, 2016 on the fight against money laundering and the financing of terrorism; Law No. 061-2008/AN of November 27, 2008 on the general regulation of electronic communications networks and services; Decree No. 2020-0099/PRES/PM/MSECU/MJ/ MINEFID of February 14, 2020 on the creation, powers, organization and operation of the Central Brigade for the Fight Against Cybercrime; Decree No. 2013-149/PRES/PM/MDENP/MEF/MJ of March 21, 2013 defining the obligations of electronic communications service operators with regard to the retention of traffic and location data; Decree No. 2013-1053/PRES/PM/MEF/MATS of November 11, 2013 creating the National Information Systems Security Agency.	The fight against cybercrime has been the subject of a series of texts tending to frame it. In terms of legislative and regulatory texts, we note the adoption of a certain number that regulate and punish cybercrime offences.
Cabo Verde	Decree-Law, nº 9/2021 of 29 January, created the cybersecurity legal regime and computer security incident response team; Creation of the Cybercrime Law No. 8/IX/2017 of March 20 - relating to international cooperation in criminal matters, and collection of evidence in electronic form; General Data Protection Regime by Law No. 41/VIII/2013 of September 17; Electronic Commerce Law; Public Key Infrastructure Act; Digital Signature Law; Electronic Identity Law.	Cabo Verde establishes the criminal, material and procedural provisions, as well as provisions relating to international cooperation in criminal matters, relating to the fight against cybercrime and the collection of digital evidence and electronic data.

Member States	Laws and Regulatory Provisions	Comments
Cote d'Ivoire	Law No. 2013-451 of 19 June 2013 on the fight against cybercrime; Law No. 2013-450 of 19 June 2013 relating to the protection of personal data; Law No. 2011-546 of 30 July 2013 on electronic transactions governing electronic commerce, advertising, etc.; Ordinance No. 2012-243 governing all ICT activities from or to Côte d'Ivoire; and Decree No. 2011-476 of 21 December 2011 identifying subscribers of telecommunications services providers.	This law defines specific offences related to ICTs, intellectual property infringements, illegal acts on electronic communication networks and the responsibilities of online service providers. It adapts traditional offences to ICT and clarifies criminal procedure for cybercrime. In addition to this law, other laws, regulations, and decrees have been issued, in addition to the penal code, by the Ivorian authorities with the aim of regulating and securing Ivorian cyberspace.
Gambia	Information and Communications Act (ICA), 2009; Evidence Act, 1994; Copyright Act, 2004; Criminal offences bill, 2020; Criminal Code (1933, as last amended by Act No. 18 of 2010); Criminal Procedure Code (1933, as last amended by Act No. 5 of 2005; and	The Council of Europe and OCWAR-C supported the Gambian Ministry of Justice and Ministry of Communication Digital economy in the preparation of a draft Cybercrime Bill, which was finalized in December 2019 and opened for public consultation until January 2020. The Minister of Communications and Digital Economy is still working on finalizing the cybercrime bill.
Ghana	Cyber Security Act, 2020 (Act 1038); National Information Technology Agency Act (NITA), 2008 (Act 771); Electronic Transactions Act, 2008 (Act 772); Electronic Communications Act, 2008 (Act 775); Data Protection Act, 2012 (Act 843); Economic and Organized Crime Office Act, 2010 (Act 807); Anti-Money Laundering Act, 2020 (Act1044); Anti-Terrorism Act, 2008 (Act 762); Payment Systems and Services Act 2019 (Act 987); Mutual Legal Assistance Act, 2010 (Act 807); Banks and Specialised Deposit-Taking Institutions Act 2016 (Act 930); Non-Bank Financial Institution Act 2008 (Act 774).	The Cybersecurity Act seeks to promote the development of cybersecurity and to provide for related matters. It also established the Cyber Security Authority (CSA) to regulate cybersecurity activities. The board of the authority is constituted by the Ministers of Communication, Defense, National Security, and the Interior. For good coordination in cybersecurity incidents, the authority is required to establish sectoral computer emergency response teams (CERTs), including for the banking and finance sector.
Guinea	Law L/037/AN/2016 on cybersecurity and the protection of personal data; Law L/035/AN/2016 on electronic transactions; Law No. 059/AN/2016 on the Criminal Code; Law L/2021/024/AN of 17 August 2021 on the fight against money laundering and the financing of terrorism.	The laws define the rules and mechanisms to fight against cybercrime and thus create a favorable, conducive and secure environment in cyberspace, but also to allow the Republic of Guinea to comply with its community and international commitments on cybersecurity. It also promotes the modernization of the use of ICT as well as support the fight against ML/TF
Liberia	Fraud Act, 2012 – criminalizes wire fraud and mail fraud. AML/CFT Preventive Measure for Proceeds of Crimes Act 2021- recognizes fraud as a predicate offense to ML. Telecommunications Act 2007- provides means for Law Enforcement Agencies to obtain digital evidence.	Liberia as a Country does not have a direct legislation on Cybercrimes. A bill (Cybercrime Act) has been submitted to Parliament for enactment into law. However, Liberia relies on other pieces of legislations to address issues surrounding cybercrimes.

Member States	Laws and Regulatory Provisions	Comments
Nigeria	Cybercrime (Prohibition, Prevention, etc.) Act, 2015; Economic and Financial Crimes Commission (Establishment) Act, 2004; the Advanced Fee Fraud and Other Related Offenses Act, 52 (2006); the Money Laundering (Prohibition) Act, 2011 as amended in 2013; the Nigerian Evidence Act, The Criminal Code Act, The Penal Code Act, The Terrorism (Prevention) Act, 2013, and the National Identity Management Commission Act, 2007	With the advent of the Cybercrime Act in 2015, Nigeria became more legally equipped in the fight against cybercrime activities. However, it may not be adequate to discuss the Cybercrime Act 2015 without throwing some light on the enabling laws that were in existence for controlling cybercrimes (i.e., the EFCC ACT, AFF Act, etc) before the Act was enacted.
Senegal	Law 2008-08 on electronic transactions and to promote ICT trade; law 2008-12 of January 25, 2008, on the protection of personal data; law 2008-11 of January 25, 2008 on cybercrime;	As early as 2008, the country adopted a normative framework to combat cybercrime and regulate the information system. These laws provide the framework on electronic transactions, data processing, promote the development of trade in the ICT sector, and the protection of personal data, as well as regard for fundamental human rights and freedoms.
Sierra Leone	The Telecommunications Act 2006; Cybersecurity and Cybercrime Act 2021; Anti-Money Laundering and Combating of Financing of Terrorism Act 2012; National Security and Central Intelligence Act 2002.	This Act provides a framework to curb cybercrime and money laundering and terrorist financing, protect critical national information structures and computer systems, collection of electronic evidence to investigate and prosecute cybercrime, protect national security, conduct of covert intelligence operations throughout the territory of Sierra Leone, and facilitate international cooperation.

49. Table 3.1 depicts the legal and regulatory provisions put in place by competent authorities in member States to combat cybercrime. Except for a few that still rely on other related laws to fight cybercrime, most member States have standalone laws on cyber security and cybercrime. The applications of this laws to detection, investigation and prosecution have focused principally on the predicate offence, ignoring the need for parallel detection and investigation of the money laundering aspect of the cases.

Institutions Responsible to the Fight Against Cybercrime in West Africa

Benin

50. The lead agency on the fight against cybercrime is the Central Cybercrime Repression Office (OCRC), placed under the authority of the Director of the Judicial Police, is responsible for ensuring that all preventive measures are considered in the fight against cybercrime, including offenses relating to computer systems, as well as the management of databases. It also provides technical assistance to services requiring its expertise, conduct training, etc. The FIU is also responsible for the analysis of information and providing the origin, destination, nature of any operations, etc. Other institutions responsible for fighting cybercrime are the Ministry of Economy and Finance, the Ministry of Justice, the Ministry of the Interior and Public Security, the National Agency for the Identification of Persons (ANIP), the Information and Digital Systems Agency, the Digital Development Agency(DNA), and the Beninese Agency for Universal Electronic Communications and Postal Service(ABSUCEP).

Burkina Faso

51. The Ministry of Digital Transition, Posts and Electronic Communications (MTDPCE) ensures the implementation and monitoring of government policy in terms of development of the digital economy, posts and digital transformation. The National Intelligence Agency's main missions are to collect and exploit information recognized as being of vital interest for security. The Commission for Computing and Liberties (CIL) is the supervisory authority responsible for ensuring the protection of personal data, by informing all data subjects and data controllers of their rights and obligations and by controlling the use of information technologies and communication applied to the processing of personal data. The National Information Systems Security Agency (ANSSI) is responsible for managing the security of information systems and cyberspace. The Regulatory Authority for Electronic Communications and Posts (ARCEP) is responsible for monitoring compliance with the regulations in force in the electronic communications sector, managed and assigned radio frequencies and monitor the conditions of use, and monitor the development of technologies and prescribe measures to stimulate and facilitate investment in the electronic communications sector. The National Financial Information Processing Unit (CENTIF) is responsible for collecting, processing and disseminating information to the competent authorities or other Financial Intelligence Units. Other state actors are the General Directorate of the National Police; the General Staff of the National Gendarmerie; the General Directorate of Transmissions and IT; the Central Brigade for the Fight against Cyber Crime; the Special Brigade for Anti-Terrorist Investigations and the Fight against Organized Crime; the Office of National Identification; and the Ministry of Justice.

Cabo Verde

52. Cape Verde continues to invest heavily in a knowledge, informative, innovative and prosperous society, as well as investing and strengthen ICT institutions, namely the Multisectoral Regulatory Agency for the Economy, the Ministry of Digital Economy, the National Council for the Development of ICT at the National Commission for Data Protection and providing quality technological infrastructures, as well as in the training of human resources. The government approved the National Cybersecurity Strategy (ENCS) and created the National Cybersecurity Nucleus (NNCS). The government also, established the Computer Emergency Response Team and the Central Brigade to Combat Cybercrime and Terrorism of the Judiciary Police - BCCCT in 2021.

Côte d'Ivoire

53. State actors that are in the fore front in fighting cybercrime are the Directorate for tracing IT (DITT) , an entity of the National Police with specialized services responsible for telecommunications infrastructures and providing technical assistance to law enforcement and judicial services. This structure was set up in May 2007 as part of the fight against cybercrime. The Computer Emergency Response Team (CI-CERT) is set up by the Telecommunications Regulatory Authority in June 2009. It is an emergency alert and response center for cyber-attacks occurring in Ivorian cyberspace. Equipped with specialized human resources in information security systems, the team offers proactive and reactive technical assistance to companies and individuals during security breaches. As the coordination center with a network of global partners, it is the national focal point for IT security monitoring, detection and alerting of security incidence. The forum on the fight against Cybercrime is also a partnership agreement signed in 2011 and updated in 2014, between the General Directorate of the National Police and CI-CERT. It is an entity integrated into the DITT of the National Police, which ensures its management. The PLCC is another structure in charge of the fight against cybercrime in Côte d'Ivoire and is supported in the execution of its missions, by the CI-CERT and the Computer Forensic Lab of the DITT. In addition to criminal investigations that cover the search for and provision of justice for suspected cybercriminals.

54. Other state actors in the fight against cybercrime are the FIU, the Criminal Asset Management and Recovery Agency (AGRAC), the Directorate of Economic and Financial Police, the Economic and Financial Crime Unit "is a" criminal court of first instance, specializing in economic and financial crime, the Public Prosecutor's Office, the criminal Police Directorate, and the research sections of the National Gendarmerie. The nonstate actors comprise of the telecommunication companies, mobile phone operators, internet service providers and financial institutions.

The Gambia

55. The Ministry of Communications and Digital Economy oversees the development and implementation of the laws, regulations, and strategy for the ICT sector. The telecommunication sector, a key component of Gambia's critical national infrastructure, is largely regulated by the Public Utilities Regulatory Authority ('PURA'). The PURA sets up the Gambia Computer Security and Incident Response Team (the gmCSIRT). The gmCSIRT supports all Critical Information Infrastructure (CII) holders in the Gambia. The Attorney General's Chambers and Ministry of Justice, through the Criminal Prosecution Department is responsible for commencing, taking over, and continuing or discontinuing criminal proceedings against or in respect of any offender. Judiciary of the Gambia holds the overall mandate for adjudication of disputes through the due process of law, administration of courts, registries, processes, directives & procedures and enforcement of decisions, orders, rulings and judgments. The Gambia Police Force is also at the forefront countering cybercrimes. The police had benefitted through the OWAR C project an equipped Digital Lab and some (15) police officers were trained on how to conduct digital forensic investigation on electronic devices and networks in other to successfully conduct cybercrimes investigations. The FIU is mandated to carry out analysis, disseminate, or shelve Suspicious Transaction Reports (STRs), seeking/responding to information request. The Gambia established a Cyber Security Alliance (GCSA) in 2017 and develop a National Cyber Security Plan (2020 to 2024) which serves as a guide to protect the nation's information systems, critical infrastructures and Gambia's cyberspace in general.

Ghana

56. The state actors responsible for fighting cybercrime in Ghana are the Financial Intelligence Centre (FIC), the Cyber Crime Unit in the Criminal Investigation Department of the Ghana Police Service, the Economic and Organised Crime Office (EOCO), the National Cyber Authority, the National Intelligence Bureau (NIB), the National Communications Authority (NCA), the Bank of Ghana (BoG), and the Securities and Exchange Commission (SEC). The Ministry of Communications and Digitalisation (MOCD), using the Ghana Card as a source document, announced the re-registration of Subscriber Identification Module (SIM) cards offered by the telecommunications companies in the country. The National Cyber Security Centre of the MOCD is responsible for capacity building and awareness creation on cyber hygiene and cybersecurity for the general public.

Liberia

57. The Liberia Telecommunications Authority (LTA) is responsible to license and regulate telecommunications operators, service providers and monitors their performance, implement policies and strategies with respect to telecommunications services and provide the policy agenda for the development of ICT and Telecommunications in Liberia. The National Security Agency (NSA) has a cybercrime lab but the guidelines for reporting and accessibility to the public to report cybercrime cases is unknown. The Liberia national Police (LNP) has a section

to handle cybercrime cases but is inactive with low manpower, lack of cybercrime knowledge and tools. The Financial Intelligence Agency (FIA) serves as the central, national agency responsible for the receipt and analysis of suspicious transactions or activities reports. The Liberia Cyber Crime Prevention and Mitigation Agency (LCCPMA) as an institution also has vast international support networks, some of which include partnership with the Global Cyber Alliance in 2020, and with the Global Forum on Cyber Expertise (GFCE) in 2021, etc.

Nigeria

58. The institutional frameworks discussed are the Nigerian Financial Intelligence Unit (NFIU), the Special Control Unit against Money Laundering, and the Nigerian Cyber Crime Working Group. Cybercrime is a term that broadly describes criminal activity in which computers or computer networks are a tool, target, or place for criminal activity. With easy access to the internet, cybercrime has become increasingly prevalent among our youth today. What is more worrisome is the rate at which their victims fall for their fraudulent tricks. What is even more worrisome is that these youths have mastered the act of cybercrime.

Senegal

59. In order to contain the impacts of cybercrime and to question the executives and the tools necessary to understand the digital environment, Senegal set up a national cybersecurity school with a regional vocation in 2018. This school mainly aims to provide training of experts in cybersecurity and to constitute a pole of reference in Africa. Finally, to adapt their organizations and equip themselves with the means to respond effectively to the security challenge posed by cybercrime, the National Police and Gendarmerie have set up specialized services in the fight against cybercrime. These are respectively the Special Cybersecurity Division (DSC) and the Digital Platform for the Fight against Cybercrime (PNLC).

Guinea

60. The National Agency for Information Systems Security (ANSSI) is a major player in cybersecurity and provides expertise and technical assistance to regulators, law enforcement agencies and companies. It provides a monitoring, detection, alert and reaction service to cyber-attacks. The Cybercrime Unit of the Central Directorate of the Judicial Police is also, a body set up by Minister of Security and Civil Protection and plays a very important role in the fight against cybercrime. The Criminal Investigations Division of the Central Directorate of the Judicial Police is also responsible for cybercrime investigations and works closely with all prosecutors in the country. Other state actors are the postal and telecommunications regulatory authority; the National Agency for the Fight against Corruption and the Promotion of Good Governance (ANLC); the financial intelligent Unit; INTERPOL Central Network (NCB); and the prosecutors' office.

Sierra Leone

61. The Cybercrime Unit investigates all reported cybercrime cases. The National Telecommunications Commission (NATCOM) is the primary regulator of all Mobile phone services and internet service providers (ISPs). It issues directives and guidelines and work with cybercrime investigators and the FIU. The FIU provides financial analysis and financial intelligence reports on ML/TF activities if any. Other state actors are the National Civil Registration Authority (NCRA), the Transnational Organized Crime Unit (TOCU), the Central Intelligence and Security Unit (CISU), the Sierra Leone Police, and the Director of Public Prosecutions (DPP). In addition to these state actors, there are interagency collaboration initiatives such as National Cybersecurity Advisory Council, the National Cybersecurity Technical Working Group, the Financial Crimes Working Group and the Joint Intelligence Committee. These bodies are made up of stakeholders from law enforcement agencies, regulatory institutions, security and intelligence gathering institutions and the relevant line ministries. The main objective of these interagency set up is

to achieve a high level of cooperation and collaboration in order to ensure a safe cyber environment. Sierra Leone also, "develop" a National Cybersecurity and Data Protection Strategy (2017 – 2022). The strategy categorises cybercrime into cyber-dependent crimes (crimes committed with the use of ICT devices only, where the devices are both the tool for committing the crime, and the target of the crime, while the cyber-enabled crimes deal with old fashioned crimes which due to the use of ICT devices and network has increased in scale or reach.

Ratification of International Instruments

62. In line with global standard requirements particularly, the FATF Recommendation 36 on International Cooperation (i.e., the implementation of international instruments), "…. *countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001;* ….". this requirement is known as the Budapest Convention.

63. Like the Budapest Convention, the African Union Convention on Cyber Security and Personal Data Protection (June 2014), known as the Malabo Convention, encourages it membership to ratify and implement the provisions set out in the convention and as agreed by the membership. However, mechanisms for inter-institutional and international cooperation are weakly regulated by legislation, as such, the challenges to criminal investigation and prosecution in this area remain significant in some countries. Even though almost all West African countries have a national strategy in place to combat cybercrime, some countries are yet to ratify the Budapest and Malabo Conventions to strengthen regional cross border cooperation.

64. Below is the status of ratification and implementation of the two complementary instruments (conventions) to help member States strengthen their framework to prevent and disrupt cybercrime.

Figure 3.1: Ratification of International Instruments

BUDAPEST	MALABO
Cabo Verde Senegal Ghana Nigeria	Cabo Verde Cote d'Ivoire Ghana Guinea, Niger Senegal Togo
Signatories and Invited to Accede Benin Burkina Faso Cote D'Ivoire Niger Sierra Leone	Signed but yet to Ratify Comoros Gambia Ghana Guinea Bissau Sierra Leone Sao Tome & Principe Togo

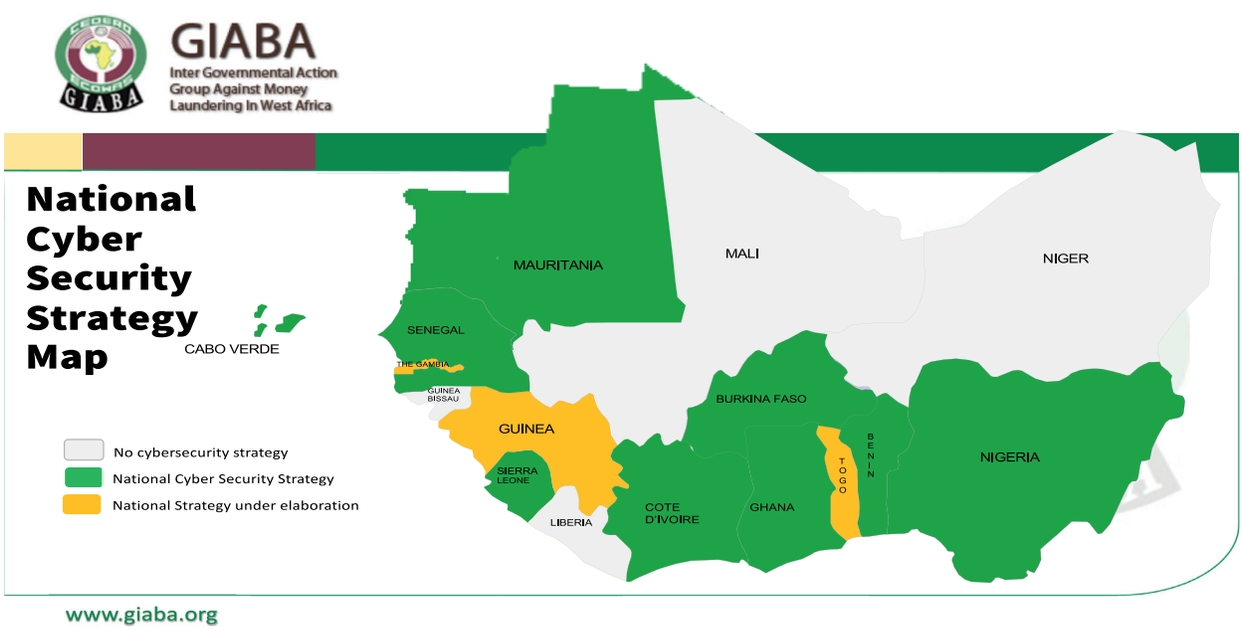
Source: OCWAR-C

65. Figure 3.1 above shows that 4 countries, Cabo Verde, Ghana, Nigeria and Senegal are parties to the Budapest Convention, while 5 other countries, Benin, Burkina Faso, Cote d'Ivoire, Niger and Sierra Leone are now signatories and invited to accede to the convention, bringing the number of West African countries to 9 that have taken measures to implement the Budapest convention on cybercrime. In the case of the Malabo Convention, only Ghana and Togo have fully implemented the requirement (signing and ratifying) of the convention in West Africa. In addition to Ghana and Togo, 5 other countries have only ratified (Cabo Verde, Cote d'Ivoire, Guinea, Niger, and Senegal) without signing the convention, while another 3 countries signing (Gambia, Guinea Bissau, and Sierra Leone) without ratifying the convention. There are however, 2 other non-ECOWAS GIABA member States that have signed the Malabo convention but are yet to ratify it.

66. Also, the European Union project on Organized Crime: West Africa Response to Cybersecurity and fight against Cybercrime (OCWAR-C) executed by the Expertise France group worked with member States to develop national cybersecurity strategies. During the review period, 8 countries had put in place national strategies with 3 others being finalised, bringing the total to 11 out of 15 countries. The 4 other countries that were yet to develop their national cybersecurity strategies are Guinea Bissau, Liberia, Mali, and Niger. Below is the map showing the status of the national strategies.

67. At the regional level, ECOWAS issued a Directive (2010) on fighting cybercrime and the adoption of substantive criminal law and procedure to address cybercrime in member States. In addition to the directive, ECOWAS implemented the harmonisation provision, particularly, the Supplementary Act on personal data protection and to ensure confidentiality, and the Supplementary Act on electronic transaction with conditions for acceptance of electronic signature.

Figure 3.2: National Cyber Security Strategy in West Africa



Source: OCWAR-C

Legal, Regulatory and Enforcement Challenges

68. The West Africa region has made considerable effort and progress in the fight against cybercrime, alongside other predicate offences. But these effort and progress have not been free from challenges, which remain daunting and persistent as criminal device new methods and techniques to avoid being detected. A summary of the challenges are as follows.

69. Even though most of GIABA member States have taken steps to have laws to empower competent authorities in the fight against cybercrime, there are still limitation in the existing legal and institutional framework. There are grey areas that needs to be explicit where the laws exist and countries without standalone laws should speed up the process to enact one. The laws should be guided by the provisions made in both the Budapest and Malabo conventions, including accepting digital and electronic evidence in the judicial process and speeding up judicial process. The FATF Standards have also provided some requirements in the various recommendations (particularly R.3 and other recommendations dealing with preventive measures for FIs, DNFBPs and VASPs).

70. Low level of operationality of the structures and mechanisms responsible for cybersecurity and the fight against cybercrime. The establishment of a digital laboratory, equipped with high-performance tools to analyse digital evidence and making effective use of such technology throughout the criminal justice chain need to be strengthened. The roles and responsibilities of different stakeholders needs to be clearly defined and modalities of collaboration and coordination understood.

71. Expertise / knowledge of competent authorities fighting cybercrime in financial and digital investigations is still very basic / low and requires continuous training of these actors (police, prosecutors, ICT engineers, FIU analysts, magistrates and all actors in the criminal justice chain).

72. Inadequate resources (financial and material) continue to slow the fight against cybercrime as cases are often reported in numbers and the records to be considered for analysis are mostly voluminous and required both skill and manpower. For instance, where millions of records, accounts, credit cards, or personal photos are hacked, you required a good number of highly skilled personnel to complete investigation in good time.

73. Lack of awareness of the dangers of lack of precaution and inappropriate use of the cyberspace, including social media. Inadequate awareness among ICT users and victims of cyber-crimes about their rights to file complaints. Also, cybercriminals are emboldened due to the fact most victims, especially when it comes to certain offences affecting honour and dignity, refrain from filing complaints and prefer to resign themselves to their fate in order to avoid any scandal or stigma.

74. Lack of inter-institutional collaboration and international cooperation. The ratification of the Budapest and Malabo Conventions on Cybercrime is still very low and so is the benefit that comes along in terms of international cooperation and capacity building. The intensification of inter-agency cooperation for better management of information and intelligence that may lead to the detection of offences, the arrest of alleged perpetrators and their referral to the competent prosecutors' offices.

75. The complex nature of investigation required to gather evidence to prosecute cyber cases is a major hurdle. The major difficulty faced by law enforcement is in tracing of the primary source of the cyber-attack. The Cyber Crime Unit and other Law Enforcement Units are often unable to get to the source of the information even within the country and it is even more complex in situation where the cyber-attack emanated from outside the country and there is the need to rely on mutual legal assistance request.

CHAPTER 6

CONCLUSION AND RECOMMENDATIONS

Conclusion

76. Innovation and emerging technologies have changed the ways businesses are being conducted across the globe. In the same vein, organizations and institutions alike have adopted smart ways of implementing programs leading to efficiency and effectiveness. The world has witnessed significant growth from the use of these emerging technologies, whether it is financial technology, artificial intelligence, business intelligence, robotics, ChatGPT, etc.

77. However, these technologies operating within the internet superhighway known as the cyberspace is used to commit, facilitate and enable classic crimes (predicate offences to ML/TF). Cybercrime and ML/TF are inextricably linked and together pose major security challenges around the world. Generally, a high level of ICT skills is necessary to commit cybercrime and to counter it. This is, however, not the case in West Africa, where there has been a mismatch between the superior skills demonstrated by cyber criminals to that of competent authorities fighting cybercrime.

78. Although there are wide ranges of methods and techniques used by cybercriminals to launder the proceeds of their criminal activities, investigators and prosecutors have conducted few or no parallel financial investigations when cybercrime is detected. They are also confronted in many cases with the difficulty of establishing proof of the cybercrime offence, due to a lack of the required technology or equipment, ineffective integrated national coordination between AML/CFT operational units, and a lack of implementation of regional and international cooperation mechanisms.

Recommendations

79. In order to stay on course in the fight against cybercrime in West Africa whilst making it more effective and more deterrent, the following recommendations are hereby put forward for both the public and competent authorities fighting against cybercrime.

For the Public

80. Initiate and intensify awareness-raising campaigns for the general public on the modus operandi of cybercriminals and the risks associated with the use of the Internet, as well as on existing methods and techniques deployed by cybercriminals.

81. Promote the culture of cybersecurity in the region and support countries in the establishment of a legal and institutional framework in accordance with international standards currently in force.

National Authorities

82. To effectively combat cybercrime, risks must be properly assessed and understood by countries. Reliable and comprehensive statistics on the actual situation in relation to the cybercrime offence should be well documented for this purpose.

83. Set up Digital Forensic Laboratory; forensic evidence in support of police, judicial or security efforts to link an individual or individuals to a crime, providing evidence (including digital evidence), detecting and monitoring certain types of crime using financial and artificial intelligence.

84. Strengthen the operational capacities of investigators on digital investigation techniques adapted to the criminal investigation of this category of offences.

85. Bridge the gap between the legal framework and the Special AML/CFT/CFP laws to facilitate and fast track the criminal prosecution of the cybercriminal offence.

86. Establish and promote cooperation mechanisms between law enforcement agencies, stakeholders and other competent authorities.

87. In line with the FATF Standards take steps that can strengthen cross border cooperation by being part of other relevant international instruments that enable international co-operation in cybercrime cases such as the Budapest Convention on Cybercrime and the Malabo Convention.

88. Provide the relevant LEAs fighting cybercrime with sufficient resources (human, material, financial, etc.).

89. Develop a National Digital Identification Framework to safeguard Digital ID systems.

90. Promote specialized judges and prosecutors dedicated to prosecuting and adjudicating cybercrime related offences.

Regional and International Bodies / Authorities

91. Set up a Regional Forum of National Platforms to Combat Cybercrime in West Africa to allow competent authorities to network, share information and intelligence, as well as to share experiences in real-time.

92. Cooperate on the follow up and monitoring of the signing, ratification and domestication of international instruments.

93. Create a framework for cooperation between researchers and cybercrime units.

94. Build capacity in detection, investigation, prosecution and adjudication of cybercrime cases and how to follow the money, including undertaken parallel and financial investigation.

95. Support the conduct of cyber related risk assessment both at national and supranational level.

REFERENCES

ECA (2021), 'Cybercrime, A barrier to Africa's thriving digital economy', https://www.uneca.org/stories/cybercrime%2C-a-barrier-to-africa%E2%80%99s-thriving-digital-economy

FATF – Interpol - Egmont Group (2023), 'Illicit Financial Flows from Cyber-Enabled Fraud,' https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyber- enabled-fraud.html

FATF (2021), 'Opportunities and Challenges of New Technologies for AML/CFT', https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html

FATF (2022), 'Money Laundering and Terrorist Financing Arising from Migrant Smuggling' https://www.fatf-gafi.org/en/publications/Methodsandtrends/Migrant-smuggling.html

Feyen, E. et. Al (2021), 'Fintech and the digital transformation of financial services: implications for market structure and public policy', a BIA Paper No 117, https://www.bis.org/publ/bppdf/bispap117.pdf

Konellos, M. F. (2021), '*Cyber Security Challenges with Emerging Technologies'* https://www.japcc.org/articles/cybersecurity-challenges-with-emerging-technologies/

Kshetri, N. (2019), 'Cybercrime and Cybersecurity in Africa', Journal of Global Information Technology Management, https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527

OECD (2021), 'Misuse of E-Commerce for Trade in Counterfeits', https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/misuse-e-commerce-trade-in-counterfeits/EUIPO_OECD_misuse-e-commerce-trade-in-counterfeits_study_en.pdf

Onota, E. (2021), 'Globalization and Emergence of Cyber Crimes in Nigeria: the YahooBoys Syndrome', Journal of Political Sciences & Public Affairs

Sumadinata, W. S. (2023), 'Cybercrime and Global Security Threats: A Challenge in International Law', Russian Law Journal, Volume XI (2023) Issue 3

Tropina, T. (2016), 'Do Digital Technologies Facilitate Illicit Financial Flows ?', World development report, https://thedocs.worldbank.org/en/doc/396751453906608518-0050022016/original/WDR16BPDoDigitalTechnologiesFacilitateIllicitFinancialFlowsTropina.pdf

Annex A:

CASE ANALYSIS TEMPLATE

CASE ANALYSIS TEMPLATE FOR TYPOLOGIES PROJECT ON MONEY LAUNDERING AND TERRORIST FINANCING LINKED TO CYBERCRIME IN GIABA MEMBER STATES

Name of Country_____ Case No._____

a. **Brief Facts of the case (including what prompted the commencement of the investigation and status of the case as at the date of reporting):**

b. **Techniques/methods**

Please indicate with the case example the occurrence of any of the following techniques/methods/schemes and use of any instruments listed:

B1. Corruption: Please, report the incidences of corruption related to this case, if any (bribery/attempted bribery of officials, third parties, possible influence by politically exposed persons (PEPs) to influence investigating officials or private sector compliance staff in banks being bribed or influenced to allow illicit proceeds from cybercrime being laundered or used for terrorist financing or proliferation financing purposes

B2. Cash couriers / currency smuggling: Concealed movement of money suspected to have been derived illicitly from cybercrime and thereby avoiding transaction / cash reporting measures.
B3. Structuring (smurfing): Numerous transactions involving illicit proceeds from cybercrime (deposits, withdrawals, transfers) high volumes of small transactions and sometimes numerous accounts to avoid detection threshold reporting obligations

B4. Purchase of valuable commodities (gems, precious metals etc.): Use of proceeds from cybercrime to purchase instruments to conceal true ownership or move value without detection

B5. Purchase of valuable assets (landed properties/real estate, vehicles, etc): Investment of proceeds of cybercrime in high-value negotiable goods to cover up the criminal source of the proceeds.

B6. Trade-based money laundering and terrorist financing: Manipulation of invoice and use of trade finance routes and commodities to launder the proceeds of cybercrime

B7. Wire transfers: Transfer of illicit proceeds of cybercrime electronically between financial institutions from outside of the country or from the country to another country

B8. Investment in capital markets: Incidence of trying to cover up the source of proceeds of cybercrime through investment in the capital market and other negotiable instruments

B9. Business investment: The mingling of the proceeds of cybercrime with legitimate business monies in order to cover up the source of the funds.

B10. Alternative remittance money services: The use of informal money service mechanisms to transfer or receive the proceeds of cybercrime

B11. Use of nominees, trusts, family members or third parties etc: Transfer of proceeds of cybercrime to nominees, trust, family members or third parties by drug traffickers / organised criminals to protect their identities and/or for safe keeping/laundering.

B12. Use of DNFBPs: The use of professionals such as accountants, real estate agents, lawyers, etc., to launder the proceeds from cybercrime

B13. Use of debit cards, credit cards, other payment cards, cheques, promissory notes etc: The use of cards, cheques, promissory notes to receive/make payment or launder the proceeds of cybercrime within national jurisdiction or to another jurisdiction.

B14. Currency exchanges / cash conversion: use of the formal or informal currency exchange system to launder/transfer proceeds of crime from cybercrime

B15. Commodity exchanges (barter): Direct exchange of commodities (legal or illegal) to conceal the origin of value being criminal proceeds from cybercrime

B16. Gaming activities (casinos, gambling etc.): Use of proceeds of cybercrime to, for example, buy winning tickets from legitimate players; using casino chips as currency for criminal transactions; using online gambling to obscure the source of criminal proceeds.

B17. Abuse of non-profit organizations (NPOs): Use of NPOs to transfer proceeds of crime from cybercrime in or out of the country

B18. Use of shell companies/corporations: Incidences of use of shell companies to cover up the identity of persons involved in crime in the cyber / virtual assets industry

B19. Use of foreign bank accounts: Movement of proceeds of crime from cybercrime from point of high vigilance to a point of low vigilance (in or out of country)

B20. Identity fraud / false identification: use of false identity by persons involved in the case of cybercrime to obscure identification of those involved in many methods of money laundering (if possible, provide some information as to how they obtained the false identity – corruption, intimidation, financiers, etc)

B21. Virtual Assets (VA) and Virtual Assets Services Providers (VASP): Use of illicit proceeds from cybercrime and VA activities and using cyberspace and VA space to launder or finance terrorism or proliferation

B22. Terrorist Financing: Use of proceeds of cybercrime to finance or facilitate terrorism and terrorist activities (in or out of country)

B23. Please, summarise the outcome of investigation and/or prosecution of the case
B24. Please, provide any additional information on any technique/method not adequately covered above.

****

Complexe SICAP Point E,
Immeuble A, 1er Etage
Avenue Cheikh Anta Diop x Canal IV
B.P. : 32 400 Dakar - Ponty (Sénégal)
Standard : (+221) 33 859 18 18
Fax : (+221) 33 824 17 45
www.giaba.org