MONEY LAUNDERING CASE

By Ms Amivi EZA
SECRETARY GENERAL OF CENTIF-TOGO
hopeeza@gmail.com
+228 90 12 10 07

INTRODUCTION

The Republic of Togo is a member state of the West African Economic and Monetary Union (WAEMU, UEMOA in french) community, which is composed of 8 member states.

The WAEMU countries use the same currency, which is the CFA franc and one banking regulator, the central bank of west african states called BCEAO.

The ML/FT regime of Togo is based on WAEMU's Directive, adopted in 2015 by its council of Ministers, in line with FATF's revised standards.

INTRODUCTION

- The Republic of Togo's FIU (CENTIF-Togo) is an administrative FIU, operational since 2009 and it has been an Egmont Group member since july 2013.
- The FIU is the central actor of the AML/CFT framework. It shares information with the other competent autorities such as law enforcement agencies and tax authority. Recently, an information shared with the tax autorithy lead to an important tax recovery of $360,000 from a company.
- The country is currently under the second round of mutual evaluation, which on site visit took place in february 2021 and we have just received, at the beginning of last week, the first draft of the report.

OUTLINE

This presentation will focus on the following areas :

- ✓ NRA key findings
- ✓ ML case presentation
- ✓ Challenges

NRA KEY FINDINGS (1)

- ✓ Togo has conducted its National Risk Assessment (NRA) in line with FATF's Recommandation 1, from June 2018 to December 2019 using the world bank's tool.
- ✓ The outcomes of the NRA revealed that the money laundering level of the country is medium high.
- ✓ The main predicate offences identified are fraud especially cyber crime related, breach of trust, tax and customs fraud, corruption, drug trafficking, human trafficking and migrant smuggling.

NRA KEY FINDINGS (2)

The country's vulnerabilities are due to the following :

- non adoption of some legal texts
- disfunction and weak capacity of law enforcement agencies
- lack of knowledge on AML/CTF obligations by reporting entities
- Inadequate or non supervision of reporting entities in the area of AML / CFT
- the predominance of the informal sector and the high use of cash in the economy
- the high level of vulnerabilities of some sectors such as real estate, banking sector and the money exchange sector.

CASE N°1 : CYBER CRIME AND IT SECURITY HACK (1)

- In 2018, Mr. “A” who is a trader opened an account in bank “X” for his commercial activities as a shoes seller in a local market. This account received a fraudulent transfer from a bank of another WAEMU country for an amount of $378,000 generated from the bank’s IT system hack.
- Thankfully, due to the sending bank’s diligence, the funds were tracked and returned before Mr. “A” was able to withdraw them.
- **Bank “X” immediately filed an STR to the FIU**.

CASE N°1 : CYBER CRIME AND IT SECURITY HACK (2)

In 2019, the FIU received a second STR related to the same individual from another bank.

The fact related to this second STR are as follows :

- ✓ In 2009, Mr. “A” opened an account in a bank “Y” for his commercial activities as a shoes seller in a local market.
- ✓ Only international transfers was received into this account.

CASE N°1 : CYBER CRIME AND IT SECURITY HACK (3)

- In 2013, four years later, his wife opened an account in the same bank for business purposes.
- The account received 48 transfers for a total amount of $244,000 from 2013 to 2019. Only one deposit was made into the account.
- Surprisingly, Mr. “A” controls entirely his wife's account true a procuration. He was the one who withdrew the money transferred immediately after receipt.

CASE N°1 : CYBER CRIME AND IT SECURITY HACK(4)

- In 2014, Mr “A” created a company and opened an account for the company in the same bank “Y”.
- This third account also received transfers for a total amount of $230,000 from 2014 to 2019, and no deposits were made.
- All these facts led bank “Y” to file STR with the FIU in 2019.
- This bank collaborated very closely with the FIU and the law enforcement authorities to arrest the suspect by setting a trap for him while he was trying to withdraw a new transfer.

CASE N°1 : CYBER CRIME AND IT SECURITY HACK (5)

- The investigations revealed that Mr. “A” is the younger brother of a cyber criminal listed in the FIU’s database. He is part of cyber criminals network engaged in the Nigerian style scam (“419” scam).
- Their method is to create shell companies and use middlemen or nominees to lure their victims into very lucrative deals. Along the way, they create imaginary costs the victim is supposed to pay, like costs of study, lawyer fees, accounting, etc.
- This allowed them to generate approximately $900.000 from their victims.

CASE N°1 : CYBER CRIME AND IT SECURITY HACK (6)

- A report was sent by the FIU to the prosecutor
- Mr. “A” was prosecuted and found guilty of money laundering, fraud, organized crime and IT security hack and was sentenced in 2020 to 72 months in prison with a fine of $200,000.
- His wife was convicted of ML and sentenced to 36 months in prison with a fine of $100,000.
- About $23,000 was recovered from one of their accounts and also a car belonging to them was confiscated.

CASE N°1 : CYBER CRIME AND IT SECURITY HACK (7)

RED FLAGS - ML

1- The swift messages of the transfers were suspicious :

- ✓ For example, payment of financial services bill, Forensic Accountant Service Payment, etc.
- ✓ The suspect is not known as a financial services provider
- ✓ The reasons provided for the transfer are typical of 419 scam

2- Funding of the accounts was in one direction :

- ✓ The accounts were funded largely from transfers received from abroad whereas the reason for opening the account as provided to the bank was commercial activities. The transfers should have been sent by him for the purchase of goods
- ✓ Almost no cash or check deposit made into the account

3- Use and full control of his wife's account (beneficial owner).

AML/CTF CHALLENGES (1)

1- **Low capacity of law enforcement agencies :** Law enforcement agencies do not have sufficient skills and resources to proactively investigate money laundering or terrorism financing cases.

2- Lack of specialized jurisdiction for prosecution : There is neither a specialized jurisdiction nor a specialized jurisdiction's office exclusively dedicated to the prosecution and trial of ML/TF cases, only limited human resources are dedicated to these cases.

3- Bribery and corruption of prosecutorial officials, the lack of independence of the prosecutors and the mobility of trained human resources, also weaken the fight against ML/TF.

AML/CTF CHALLENGES (2)

4- Identification of addresses : This is a real challenge for the reliability of basic information provided on individuals and legal persons. It can encourage the creation of shell companies and It is a challenge for tracking criminals to justice.

5- Insufficient information on beneficial owners of legal persons and arrangements (Trust) : Lack of proper mechanism to collect accurate and timely information on beneficial ownership. Criminals can easily own or control interest in legal persons or arrangements in the country.

6- Lack of due diligence by mobile phone companies especially with regard to providing GPS information in response to requests from law enforcement agencies : this can slow down investigation and in prosecuting criminals.

7- High use of cash in transactions, the lack of interconnection among existing databases, and also the emergence of virtual assets are equally challenging for the AML/CTF regime of Togo.

THANKS FOR YOUR KIND ATTENTION