COMBATING MONEY-LAUNDERING AND TERRORIST FINANCING IN THE MALDIVES

Abdulla Shahuneez[*]

I. INTRODUCTION

The Maldives faces unique challenges in combating money-laundering (ML) and terrorist financing (TF) due to its geography and economy. This paper analyses the current situation, identifies root causes, discusses challenges and suggests countermeasures.

II. CURRENT SITUATION IN THE MALDIVES

A. Economic Vulnerabilities

Tourism, fishing and import/export sectors are highly vulnerable to ML due to cash transactions and complex business structures. The Maldives' geographical location and proximity to major drug-producing and transit countries make it a vulnerable transit point for narcotics.

B. Regulatory Framework

The Maldives Monetary Authority (MMA) and Financial Intelligence Unit (FIU) oversee AML/CFT efforts. The Maldives Police Service (MPS) is central to investigations, requiring even the Anti-Corruption Commission (ACC) to collaborate via Memorandums of Understanding (MOUs). The Prosecutor General's Office (PGO) and courts handle prosecutions and adjudications. Despite a significant increase in the number of Suspicious Transaction Reports (STRs) disseminated by the FIU to the MPS, the rate of successful prosecutions remains very low, with no asset attachments or arrests made in the period from 2019 to 2024. Transaction Analysis Reports (TARs) have proven more effective than STRs in leading to prosecutions and asset attachments, with a high percentage of disseminations resulting in investigations and a proportionally higher number of prosecutions and asset seizures.

Key laws include the Anti-Money-Laundering and Counter-Terrorism Financing Act (Law No. 10/2014), Anti-Terrorism Act (Law No. 32/2025), Criminal Procedure Code (Law No. 9/2016) and FIU Regulations.

C. Legal Framework

Laws provide a framework for prevention, oversight and enforcement.

D. Challenges in Anti-Money-Laundering/Counter Terrorism Financing Implementation

Lack of a national AML/CFT strategy and coordinated approach exists. There is limited use of FIU intelligence by law enforcement and an absence of ML convictions and asset confiscations aligning with risk profiles. TF investigations are stalled, indicating a lack of demonstrated effectiveness. Delayed implementation of UN-mandated Targeted Financial Sanctions (TFS) is also evident. Unidentified high-risk Non-Profit Organizations (NPOs) persist, and varying AML/CFT knowledge across financial and non-financial sectors is a concern.

1. Drug Trafficking Impact

In the last four months of 2021, 1,480 kilos of drugs were seized en route to Sri Lanka and the Maldives, with over 400 kilos seized by Maldivian authorities. Extrapolating this, approximately 1,200 kilos of drugs could be seized annually by local authorities. Major heroin smuggling routes in the region include heroin

[*] Senior Sergeant (Investigation Officer), Anti-Scam Centre / Economic Crime Investigations, Maldives Police Service.

transported from areas controlled by Afghan warlords to Pakistan, routed via sea and land to countries such as India, Sri Lanka and the Maldives.

2. Corruption and Politically Exposed Persons (PEPs)

The FIU's 2021 analysis of TARs and STRs revealed the misuse of authority and corruption by Politically Exposed Persons (PEPs), family members and associates. This includes embezzlement and influence peddling, with individuals using nominees, family members and third parties to obscure the identity of those controlling illicit funds. The 2014 Maldives Media & Public Relations Corporation (MMPRC) corruption scandal involved allegations of corruption against public officials, including the former President and Ministers.

3. National Risk Assessment (NRA) Findings

- **Overall ML risk:** "High" due to "High" threat and "Medium High" vulnerability.
- **ML threat:** "High" due to drug trafficking, corruption and organized crime.
- **ML vulnerability:** "Medium High" due to limited law enforcement capacity, cash-based economy and gaps in DNFBP regulations.
- **High-risk sectors:** real estate, money changers, NPOs, legal/accountancy professionals, precious metals dealers and the banking sector.
- **US Department of State 2016 INCSR:** Maldives as a "Monitored" jurisdiction, citing transit point concerns, limited oversight, and illicit funds from drug trafficking and corruption.
- **Major crimes generating illicit funds:** drug trafficking, corruption and organized crime.
- **Drug trafficking routes:** Sri Lanka, India, Pakistan, Iran, Bangladesh, UAE.

4. Financial Data

- **Total Seizures/Confiscations 2020-2021 (Source: Prosecutor General's Office)**
  - Drug Trafficking Offences:
    - MVR 616,220 (2020)
    - MVR 1,232,440 (2021)
  - Corruption Offences:
    - MVR 45,308,093 (2020)
    - 1 Luxury Apartment (2020)
    - Rolex Watch (2020)
    - MVR 15,420,000 (2021)

The Financial Intelligence Unit (FIU) in their Annual Report 2021 identified the misuse of authority and corruption by Politically Exposed Persons, family members and associates; misuse of public power entrusted to them for embezzlement and influence peddling. Individuals in publicly prominent positions were noted to have used nominees, family members and third parties to obscure the identity of the persons controlling the funds.

III. ROOT CAUSES OF ML/TF IN THE MALDIVES

A. Weak Regulatory Enforcement

- Limited resources and capacity within law enforcement and regulatory agencies hinder effective enforcement.
- Concerns about corruption and lack of transparency can undermine AML/CFT efforts.

B. Geographic Vulnerabilities

- The archipelagic nature of the Maldives makes it difficult to monitor and control remote islands.
- Open borders and transit routes facilitate the movement of illicit funds.

C. Economic Factors

- The prevalence of a cash-based economy creates opportunities for ML.
- Rapid development and investment projects can attract illicit funds.

D. Social and Cultural Factors

- Informal financial systems may operate outside of regulatory oversight.
- Lack of public awareness about ML/TF risks can contribute to the problem.

IV. GOOD PRACTICES AND CHALLENGES

A. Good Practices

- The Maldives has made efforts to improve its AML/CFT framework in line with international standards.
- Collaboration with international organizations and regional partners has been strengthened.
- Public awareness campaigns are being implemented.

B. Challenges

- Resource constraints, including funding, personnel and technology, remain a significant challenge.
- Capacity-building is needed to enhance the expertise of AML/CFT professionals.
- Data collection and analysis processes require improvement.

V. COUNTERMEASURES

A. Strengthening the Regulatory Framework

- Increase funding and resources for the FIU and law enforcement agencies.

- Update and strengthen AML/CFT laws and regulations.

- Implement stricter due diligence requirements for financial institutions.

B. Enhancing International Cooperation

- Strengthening the role of the INTERPOL National Central Bureau (NCB) of the Maldives in facilitating international cooperation.

- Utilizing Mutual Legal Assistance Treaties (MLATs) to exchange information and evidence with foreign jurisdictions.

- Effectively using INTERPOL notices (e.g., Red Notices for wanted persons, Blue Notices for information gathering) related to money-laundering and terrorist financing.

C. Improving Public Awareness

- Launch targeted public awareness campaigns.

- Engage with civil society organizations and the private sector.

- Implement youth education programmes about financial crimes.

D. Technological Solutions

- Deploy advanced data analytics and transaction monitoring systems.

- Explore the use of blockchain technology for transparent financial transactions.

- Improve national cybersecurity infrastructure.

VI. CASE STUDY

A. Analysis of Money-Laundering Methods in the 500K Scam

This case study analyses the money-laundering methods employed in a significant scam incident in the Maldives, highlighting the challenges in tracing illicit funds and identifying the complex networks involved.

- **Introduction**

  - This case study explores a real-world money-laundering operation uncovered during the investigation of the 500K Scam in the Maldives. The case originated with the unauthorized withdrawal of MVR 582,149 from two individual accounts, which exposed a broader laundering network that funnelled more than MVR 27 million through multiple personal bank accounts, mule operatives and crypto channels.

  - This case demonstrates how modern money-laundering operations exploit digital vulnerabilities and how law enforcement, prosecutors and courts work together to respond.

- **Background**

  - The case was initiated in February 2024 after reports of unauthorized fund transfers from the victim's accounts. The scam resulted in the fraudulent transfer of MVR 582,149 from the victim's accounts. These funds were rapidly transferred and layered through at least 16 accounts and 20+ SIM cards, indicating a pre-planned laundering network.

- Investigations revealed links to broader scam activities, and laundering techniques included layering via transfers, ATM withdrawals, purchasing goods and cryptocurrency conversion (USDT).
- Scam cases represent a significant financial crime threat in the Maldives, resulting in substantial losses to the public.
- In the past year, total losses from scam cases reached MVR 2,402,618.81 and $350,824.68.
- The first quarter of this year saw losses amounting to MVR 13,761,259.6, indicating a potential increase in scam-related money-laundering.

- **Objectives**
    - To detail the methods used to launder funds obtained through the scam.
    - To trace the flow of illicit funds through various accounts and transactions.
    - To identify the layering techniques used to obscure the origin and destination of the money.
    - To assess the challenges in recovering the laundered funds.

- **Money-Laundering Methods (MO)**
  The operation was built on a multi-step strategy designed to steal, transfer and clean funds without raising suspicion:
    - *Phishing & Credential Theft:* Victims were tricked into revealing banking credentials via fake job ads, phishing links or investment schemes.
    - *SIM Swapping and OTP Interception:* Using forged ID cards, the perpetrators duplicated SIM cards registered to victims. This allowed them to intercept OTPs and login verifications for bank apps and mobile wallets.
    - *Unauthorized Bank Access:* Access was gained to multiple victim accounts, where transfers were quickly initiated to mule accounts under control of the network. Amounts like MVR 250,000 and MVR 557,149 were transferred from victim accounts.
    - *Layered Transactions through Fake or Rented Accounts:* Funds were structured into smaller chunks (e.g., MVR 5,000–50,000) and transferred across 16+ accounts. Some accounts were opened using fake names; others were rented from low-income individuals promised commissions.
    - *Rapid Withdrawal and Dispersal:* The network attempted to immediately withdraw or use the laundered money via ATM, POS purchases or cash handovers. In some cases, funds were moved across 8–9 accounts within hours.
    - *Use of Digital Payment Platforms:* Transactions were routed through mobile apps and social media-based payments, using vulnerabilities in e-wallet KYC systems.
    - *Cross-Border Transfers:* A portion of the stolen funds was traced to international accounts, pointing to a transnational element and possible integration into foreign financial markets.

- **Flow of Funds & Timeline**
    - *Initial Fraudulent Transfers:* 12 February 2024, 13:50–14:30.
    - *First-layer Transfers:* Executed within 2 hours.

  - *Cash Withdrawals / Goods Purchases:* Initiated within the same day.
  - *Crypto Conversion:* Completed via a third-party merchant by next day.

- **Laundering Techniques in Detail**
  - *The Structuring (Smurfing):* The laundered funds were broken down into smaller transfers to avoid bank scrutiny.
  - *Account Layering:* Over 21 documented transactions showed deliberate layering through various accounts to obscure the audit trail.
  - *Fake Identity Use:* One highlighted case involved a fraudulently named account (Mohamed Hussain) used to process over MVR 582,000.
  - *Mobile Banking Exploitation:* OTPs and access codes were obtained from compromised SIMs. Several transfers occurred moments after unauthorized logins, indicating precise coordination.

- **Police Investigation Process**
  - *Complaint Received & Financial Tracing Initiated:* Victim reports triggered a rapid tracing of outgoing transfers and ATM transactions.
  - *Account Freezes & Interagency Alerts:* Immediate bank coordination led to freezing over MVR 7 million in suspect accounts.
  - *Telecom & Device Forensics:* SIM ownership and duplication data were retrieved and cross-referenced with IMEI logs and login IPs.
  - *Suspect Identification:* Linked accounts and phone records were used to identify key suspects.
  - *Arrests Made:* 8 suspects were arrested, including:
    - 2 primary coordinators (organized logistics and crypto transfers)
    - 3 money mules who received and withdrew funds
    - 2 individuals who opened accounts using forged IDs
    - 1 digital payment intermediary

- **Prosecution and Court Proceedings**
  - *Jurisdiction:* The case was heard under the Maldives Criminal Court, which has original jurisdiction over offences under the Penal Code, Anti-Money-Laundering and Counter-Terrorism Financing Act (Law No. 10/2014), and the Evidence Act.
  - *Charges:* The suspects were charged with:
    - Money-laundering (under the AML/CFT Act)
    - Unauthorized access and fraudulent transfer
    - Identity fraud and use of forged documents
    - Obtaining property by deception

- **Prosecution Strategy**
  - *Evidence Submission:* Transaction logs, SIM registration records, forensic reports from bank apps and IP logs, and CDR data.
  - *Witness Testimony:* Police investigators, telecom reps, bank compliance officers.
  - *Digital Evidence:* Crypto purchase receipts, OTP logs, app activity records.
- **Outcome (Current Status)**
  - Proceedings are ongoing.
  - Further investigations continue regarding crypto trail and potential foreign links.

How ML Cases Are Handled in the Maldives: Investigation-Prosecution-Court

Stage	Description
Police Investigation	Initiated by victim complaint or STRs. FIU alerts, KYC violations, and CDR/IP analysis are used to trace laundering.
Account Freezing	Law enforcement issues urgent freeze orders; coordination with MMA and banks is critical.
Prosecutor General's Office (PGO)	Reviews evidence under the AML/CFT Act. Prepares formal charges and court submissions.
Criminal Court	Hears cases under relevant financial and criminal statutes. Accepts digital forensics and foreign evidence.
Asset Recovery	If convicted, court may order recovery, confiscation or restitution of laundered assets.

- **Challenges**

  Investigating and prosecuting the 500K Scam presented multiple layers of operational, technical and legal challenges, including:
  - *High Complexity of the Operation:* The case involved multiple individuals, over 16 accounts, layered transactions and SIM duplication, making it logistically complex to trace the full money trail and coordinate freezes in time.
  - *Difficulty Identifying Ultimate Beneficiaries:* Layering techniques, third-party mule accounts and forged identities made it difficult to trace the real owners and end-users of the laundered funds.
  - *Use of Social Media to Obscure Transactions:* A portion of the funds was spent on goods and services coordinated via social media platforms, making it difficult to confirm the value trail or identify vendors who accepted illicit payments.
  - *Delayed Victim Reporting:* By the time most victims reported the fraud, the funds had already passed through multiple layers, often withdrawn or converted, reducing recovery prospects.
  - *Lack of Integrated AML Tools in Banks:* Many banks did not have automated monitoring or alert systems to detect suspicious transaction patterns or high-risk account activity in real time, delaying escalation.
  - *Anonymous SIM Registrations and Weak Telecom Controls:* The ability to register duplicate SIMs without biometric verification enabled SIM hijacking and unauthorized access to mobile banking apps and OTPs.
  - *Forgery and KYC Weaknesses:* Suspects used forged identity documents to open multiple accounts, bypassing weak e-KYC procedures and enabling rapid setup of mule accounts.

  - ◦ *Cross-Border Crypto Conversion:* The use of USDT (Tether) to move funds out of the formal financial system complicated jurisdiction and blocked local recovery options.

- **Recommendations**

To strengthen the national response to money-laundering and prevent future incidents like the 500K Scam, the following strategic measures are recommended:

  - ◦ *Strengthen e-KYC and Identity Verification:* Mandate biometric verification, secure digital onboarding and enhanced due diligence for high-risk individuals to prevent the misuse of fake or forged identities in opening bank and telecom accounts.

  - ◦ *Integrate Real-Time AML Monitoring Systems:* Require all banks and mobile wallet providers to implement AI-driven monitoring tools capable of detecting unusual transaction patterns, rapid layering and account behaviour anomalies.

  - ◦ *Enforce Robust SIM Registration and Telecom Oversight:* Enact stricter telecom regulations to prevent anonymous SIM issuance and enable real-time alerts for SIM swaps. Telecom operators should integrate SIM activity monitoring with financial crime intelligence systems.

  - ◦ *Enhance Cross-Sector Information Sharing:* Establish formal, real-time communication protocols among the FIU, law enforcement, banks and telecom providers to ensure timely action on suspicious transactions and fraud indicators.

  - ◦ *Expand Public Awareness Campaigns:* Launch nationwide education initiatives on financial scams, phishing risks, OTP protection and money mule recruitment. Target both the general public and vulnerable populations often exploited in scam networks.

  - ◦ *Regulate Cryptocurrency Access and Exchanges:* Bring crypto on-ramps and exchanges under AML/CFT oversight, requiring KYC compliance, transaction reporting and cooperation with local authorities for cross-border investigations.

VII. CONCLUSION

The 500K Scam case highlights the evolving sophistication of money-laundering operations in the Maldives. It revealed how criminals exploit digital platforms, identity loopholes and institutional blind spots to rapidly move and conceal illicit funds. The use of layering techniques, mobile banking manipulation, and cryptocurrency conversions posed significant challenges to investigation and recovery efforts.

Through direct involvement in this case, I witnessed the critical importance of fast, coordinated interagency action, proactive financial surveillance and robust legal frameworks to combat money-laundering and related financial crimes.

To effectively address ML/TF threats, the Maldives must adopt a holistic approach that includes:

- Stronger regulation and enforcement mechanisms

- Technological upgrades for real-time monitoring and risk detection

- Enhanced public awareness to reduce vulnerability to scams

- International cooperation to trace cross-border transactions and crypto flows

- Dedicated resources and oversight for cases involving drug trafficking and high-risk entities like politically exposed persons (PEPs)

Given the growing volume of illicit financial flows, particularly from drug-related activities and corruption, the country must invest in capacity-building, digital infrastructure and continuous vigilance. This case underscores that safeguarding the Maldivian economy and its financial integrity will require persistent, well-resourced and collaborative efforts at all levels.

References

Financial Intelligence Unit. (2021). *Annual Report 2021*. FIU Maldives.

Maldives Monetary Authority. (2016). *Annual Report 2016*. MMA.

Maldives Police Service. (2021). *Annual Crime Report 2021*. MPS.

Prosecutor General's Office. (2021). *Prosecution Statistics 2021*. PGO.

U.S. Department of State. (2016). *International Narcotics Control Strategy Report (INCSR)*. U.S. Department of State.