ADVISORY NOTICE

NOTICE No: AF146/FIC/2

EMERGING MONEY LAUNDERING/ TERRORISM FINANCING (ML/TF) THREATS LINKED CYBERCRIME

This advisory seeks to inform all Accountable Institutions (AIs) about the evolving methods of money laundering (ML) and terrorist financing (TF) associated with cybercrime in West Africa, as identified in the recent Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) report on "Typologies of Money Laundering and Terrorist Financing Linked to Cybercrime in West Africa".

The objective is to enhance vigilance, compliance, and reporting mechanisms to mitigate these emerging threats.

Key Findings from the GIABA Report

1. **Cybercrime as a Facilitator for ML/TF:**
   - Cybercriminals exploit digital platforms to perpetrate debit/credit card fraud, email compromise scam, hacking and defrauding businesses, advance fee fraud, Ponzi scheme fraud, mobile money fraud and cyber-enabled terrorism financing through various channels.
   - Terrorist groups leverage cyber tools to solicit funds, often under the guise of legitimate charitable causes.
2. **Use of Informal Financial Systems:**
   - Unregulated money service businesses, including informal currency exchangers, are utilized to transfer illicit funds across borders, complicating traceability.
3. **Integration into Formal Financial Channels:**
   - Illicit funds are often funneled into the formal banking system through structured deposits, trade-based money laundering, and investments in high-value assets.
4. **Exploitation of Non-Profit Organizations (NPOs):**
   - Some NPOs are misused as conduits for terrorist financing, exploiting their legitimate status to mask illicit activities.

Red Flags and Indicators

In view of the above, Accountable Institutions are required to pay attention to the following suspicious activities:

- Unusual or complex fund transfers that lack a clear economic purpose.
- Frequent transactions involving high-risk jurisdictions or regions with known terrorist activity.
- Clients making donations to NPOs without a clear link to their profile or business activities.
- Use of multiple accounts to conduct transactions just below reporting thresholds.
- Sudden activity in dormant accounts, especially involving international transfers

NB: ***The red flags and indicators above are non-exhaustive and should not be considered in isolation. They can lead to suspicion of ML associated with Cybercrime.***

10TH FLOOR, CEDI HOUSE No.1 LIBERIA ROAD, ACCRA
TELEPHONE: + 233 (0) 302 – 665252
P.O. BOX GP 2674, ACCRA, GHANA
FAX: + 233 (0) 302 – 66537

Recommended Actions

1. **Enhanced Due Diligence (EDD):**
   - Apply EDD measures for clients and transactions involving high-risk countries, sectors, or activities.
2. **Strengthen Know Your Customer (KYC) Protocols:**
   - Regularly update client information and verify the legitimacy of their sources of funds.
3. **Monitor and Report Suspicious Transactions:**
   - Implement robust monitoring systems to detect anomalies and promptly report Suspicious Transaction Reports (STRs) to FIC.
4. **Staff Training and Awareness:**
   - Conduct regular training sessions to keep staff informed about emerging ML/TF typologies and red flags.
5. **Collaboration with Regulatory Bodies:**
   - Engage with FIC and other relevant authorities to share information and best practices in combating ML/TF.

ISSUED BY:
THE FINANCIAL INTELLIGENCE CENTRE
May 30, 2025

10TH FLOOR, CEDI HOUSE No.1 LIBERIA ROAD, ACCRA
TELEPHONE: + 233 (0) 302 – 665252
P.O. BOX GP 2674, ACCRA, GHA
FAX: + 233 (0) 302 – 665