TURKS AND CAICOS ISLANDS
FINANCIAL SERVICES COMMISSION

Regulating with Honesty Integrity and Transparency

Issue 2 of 2025 **Monday, 13 October 2025**

AMLSD E-NEWSLETTER

Overview

This quarter's focus is on detecting terrorist financing, particularly relating to behavioral, transactional, and symbolic indicators. Regulated entities—including Banks, MSBs, CSPs, DNFBPs, and NPOs—are expected to strengthen due diligence, staff training, and monitoring systems to address these evolving risks.

This newsletter is intended for Compliance Officers (COs), Money Laundering Compliance Officers (MLCOs), Money Laundering Reporting Officers (MLROs), Directors, Senior Management, and other relevant staff across regulated sectors who are responsible for implementing effective AML/CFT frameworks and ensuring ongoing compliance with supervisory expectations.

Why This Matters?

Recent Trends: Hate Group Financing & Why It Matters

Terrorist financing (TF) remains a dynamic and evolving threat. Extremist and hate groups are increasingly exploiting financial systems to fund their activities. These groups use coded language, symbolic references, and complex transaction patterns to evade detection. Financing methods include fundraising through NPOs, trade in high-value goods, use of cryptocurrencies, and manipulation of legal and commercial structures.

All regulated sectors—including banks, DNFBPs, NPOs, and service providers—are at risk. Recognizing red flags such as geographic risks, suspicious spending, use of hate symbols, and opaque ownership structures is essential for early detection and effective disruption of terrorist financing linked to hate and extremist groups.

Ultimately, combating TF is not just a regulatory obligation — it is a collective responsibility to protect the integrity and security of the financial system.

Top News

Detecting Terrorist Financing (TF)

Key focus: Relevant Risk Indicators & Associated Symbols

The 2021 FATF Report on Detecting Terrorist Financing provides valuable guidance, including specific risk indicators and extremist symbols that may emerge in transactions, customer due diligence, or monitoring activities.

HELPFUL LINKS

- Hate Symbols Database : [https://www.adl.org/resources/hate-symbols/search]
- UK Sanctions List: [The UK Sanctions List - GOV.UK]
- UN Sanctions Lists: [United Nations Security Council Consolidated List | Security Council]

KEY TERRORIST FINANCING RISK INDICATORS

1. **Customer Behaviour**
   - Customer reluctance to provide information on account purpose or source of funds.
   - Use of coded or extremist language in correspondence.

2. Economic Profile of the Customer
   - Newly formed legal entity receiving unusually high deposits inconsistent with founders' income.

3. Geographic Risks
   - Transfers involving countries with no clear connection to sender or beneficiary.
   - Links to high-risk jurisdictions or conflict zones.
   - Implausible reasons for cross-border fund movements, especially involving foreign nationals.

4. Spending Activity
   - Use of third parties to make purchases or transfer assets.
   - Purchases of tactical gear or communication devices without business justification.

5. Products or Services
   - Use of anonymous prepaid cards, cryptocurrencies, or high-value commodities to obscure flows.

6. Non-Profit Organisations (NPOs)
   - NPOs operating in or partnering with entities located in conflict zones where terrorist organisations are active.

7. Trade and Commercial Entities
   - Misuse of import/export businesses for value transfer (over/under-invoicing).

8. Ethnically or Racially Motivated Terrorist Financing
   - Fundraising, donations, laundering, and cryptocurrency use by extremist groups.

RECOGNIZING RELATED SYMBOLS IN FINANCIAL TRANSACTIONS

Extremist actors often use numeric codes, abbreviations, and symbolic language in payment references, account names, merchandise purchases, or donation notes. Recognizing these markers can help identify potential TF activity.

Symbol	Meaning
1 - 11 .	Aryan Knights
14 Words	“We must secure the existence of our people and a future for white children”
1488	Combination of “14 Words” and “Heil Hitler”
18	Adolf Hitler (1st & 8th letters of alphabet)
23 / 23/16	“White” / “White Power”
28	“Blood and Honour”
311	Ku Klux Klan (K is 11th letter × 3)
318	Combat 18
420 / 4:20	Adolf Hitler’s birthday
5	“I have nothing to say” (code of silence)

Symbol	Meaning
88	“Heil Hitler”
9%	Claimed projected “white population” by 2060
100%	Ethnic purity claim
AKIA	“A Klansman I Am”
FFF	“Faith Folk Family”
JOG	“Jewish-Occupied Government”
KIGY	“Klansman, I Greet You”
ORION	“Our Race Is Our Nation”
RAHOWA	“Racial Holy War”
WP / WPWW	“White Power” / “White Pride World Wide”
ZOG	“Zionist-Occupied Government”

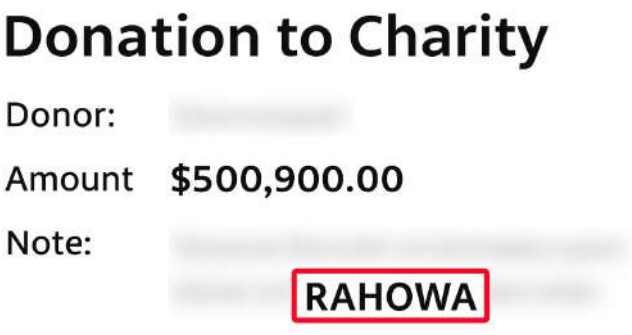
Example 1:

A bank transaction with suspicious “1488” & “ORION” code.

Date	Amount	Reference	Status
03/07/2023	$500	Janine’s Wedding	COMPLETED
03/06/2023	1.250	1488	COMPLETED
03/06/2023	$75	ORION	COMPLETED
03/05/2023	$300	Repairs	COMPLETED
03/05/2023	$50	Gas bill	COMPLETED

Example 2:

A charity receipt with suspicious “RAHOWA” code.



REAL-LIFE CASE STUDIES

Religious Non-Profit Organization and Law Firm

Description of case 1 (NPO): In what would have become a very significant legal case, a very prominent religious organization, along with its leaders, faced conviction for their involvement in providing material support to a designated terrorist organization. The foundation was found to have funneled funds to Hamas, which was alleged to have been used for various activities promoting violence and terrorism. The court proceedings highlighted the complexities of financial support in relation to national security concerns and underscored the government's efforts to combat terrorism through legal means.

What was detected? An investigation uncovered unusual grant flows and questionable partner relationships, raising serious concerns. Coded communications and financial records revealed that charitable disbursements were linked to a designated terrorist organization. Law enforcement gathered extensive evidence—including transaction data and witness testimonies—confirming that the foundation's funds were used to materially support extremist groups.
The foundation's leaders were ultimately convicted, exposing the misuse of charitable operations and underscoring the critical need for vigilance, transparency, and robust due diligence in the non-profit sector.

Description of case 2 (Bank): A neo-Nazi organization based in Europe established a network of personal and business accounts at several regional banks. The group's leaders used these accounts to collect donations, membership fees, and event payments from supporters across multiple countries. To avoid detection, payment references often included coded language and hate symbols (such as "1488" or "RAHOWA"), which are commonly associated with white supremacist ideology.

What was detected? Funds were received through direct bank transfers, online payment platforms, and cash deposits. The group pooled these resources to finance propaganda campaigns, organize rallies, and purchase materials such as banners, digital media, and tactical gear. Some funds were also used to support travel for members attending international extremist events.

The banks' transaction monitoring systems, flagged repeated use of extremist codes and symbols in payment descriptions, as well as unusual patterns of cross-border transfers and cash deposits inconsistent with customer profiles. These alerts prompted internal investigations and collaboration with law enforcement, leading to the identification and disruption of the group's financial network.

SUPERVISORY EXPECTATIONS :

ENHANCED DUE DILIGENCE (EDD)

When indicators or signs of terrorism financing (TF) risks are detected, the following measures should be implemented:

Enhanced Due Diligence (EDD): This process involves gathering and analyzing additional information about the customer, transaction, or business relationship to mitigate potential risks.

Key EDD Actions Include:

- Obtaining the source of funds and source of wealth.
- Verifying beneficial owners.
- Securing senior management approval.
- Increasing monitoring and review frequency.

EDD must be undertaken in the following situations:

1. High-Risk Customers: Customers who present a higher risk of terrorist financing or other financial crimes based on characteristics such as their occupation.

2. Politically Exposed Persons (PEPs): Individuals in prominent public positions that are linked to extremist or hate groups, that misuse their position to facilitate or conceal the movement of funds for terrorist purposes, that are involved in jurisdictions or sectors with known TF vulnerabilities.

***3. High-Risk Countries*:** Transactions with countries that are located near conflict zones or regions with active terrorist groups, have weak anti-money laundering (AML) and counter-financing of terrorism (CFT) laws, or are subject to international sanctions or with known links to terrorist organizations .

4. Complex Business Structures: Entities with complex, unclear ownership structures.

5. Suspicious Transactions: Transactions that deviate from normal patterns.

6. Onboarding High-Risk Customers: Before establishing a business relationship.

7. Executing High-Risk Transactions: Prior to executing transactions that pose a higher risk of money laundering or terrorism financing.

By undertaking EDD in these situations, regulated entities can effectively manage and mitigate risks associated with money laundering and terrorist financing.

SUPERVISORY EXPECTATIONS :

TRAINING

Ensures frontline and compliance staff are familiar with these symbols and relevant TF typologies.

AML training should occur:

1. Initially: During onboarding of new employees to ensure understanding of AML policies.

2. At least annually for existing employees with focus on updates regarding:
- Regulatory changes
- Emerging risks
- Updated internal policies and procedures

3. As needed: With significant changes to regulations, internal policies, or industry best practices.

Consistent training helps employees identify suspicious activities, manage risks, and maintain AML compliance.

An entity must provide training on:

1. Money Laundering and Terrorism Financing: This training helps employees understand and follow the rules.
2. Risk Management: Employees learn how to spot and reduce risks related to customers and transactions.
3. Compliance Procedures: Employees need to be aware and follow the organization's policies.

TRANSACTION MONITORING

Transaction Monitoring: Configuring systems to flag known extremist symbols or codes, relevant keywords and abbreviations, and number or value patterns.

Entities must conduct transaction monitoring to:

1. Identify Suspicious Transactions: Detect abnormal transactions.
2. Manage Risk: Mitigate risks related to terrorist financing and other financial crimes.

Monitoring should be:

1. Ongoing: Continuously or regularly conducted.
2. For High-Risk Customers: More frequent for those at greater risk of TF.
3. For High-Risk Transactions: Focus on large amounts, unusual patterns, or transactions from high-risk countries.

Effective transaction monitoring helps identify suspicious activities so that it may be reported to the Financial Intelligence Agency (FIA), and it helps ensure compliance with AML/CFT laws.

SUPERVISORY EXPECTATIONS :

SUSPICIOUS ACTIVITY REPORT (SARS):

Suspicious Activity (SA): Refers to any behavior or action that seems unusual, out of place, or potentially threatening. Suspicious activities may occur both internally and externally within an organization. Establishing specific reporting procedures is pivotal to efficient reporting. Employees should file internal reports directly to the Money Laundering Reporting Officer (MLRO) and avoid filtering or pre-screening Suspicious Activity Reports (SARs) through management. The MLRO is responsible for assessing the report and, where appropriate, submitting an external SAR to the FIA.

When suspicious activity is detected in either way, it's essential to respond promptly and effectively. See below a brief description for filing SARs:

Internal & External SAR Filing Obligations:

1. Upon identifying suspicious activity, staff must notify the Money Laundering Reporting Officer (MLRO) (AML/CFT Code 30(1)c).
2. Attempted transactions that are suspicious must also be reported.
3. Findings should be documented and an internal report filed for monitoring.
4. Once the MLRO has verified and corroborated the internal report, a SAR/STR must be filed with the Financial Intelligence Agency (FIA) within 24 hours (AML/CFT Code 32(1))

Completed reports should be submitted electronically to **submissions@fia.tc.**

Contact the FIA at 1-649-941-7691/3692/8429 for any queries or https://www.fia.tc/

This process can help regulated entities effectively report and monitor suspicious activities, supporting counter-terrorist financing efforts.

FINAL NOTE

Detecting TF requires a balance between vigilance and contextual assessment. It's important to recognize that the mere presence of a symbol does not confirm the existence of terrorist financing (TF). Context and supporting evidence are essential for making this assessment. By implementing a risk-based and objective approach, we can avoid perceptions of racial profiling or discrimination.

NEXT STEPS

In conclusion this quarter's newsletter on terrorist financing offers valuable insights into the evolving tactics used by terrorist groups to fund their operations, as well as the regulatory expectations placed on reporting entities. As registrants and licensees operating in a supervised and regulated environment, it is critical to translate these insights into practical action. Below are recommended next steps to enhance your organization's compliance posture:

1. Review and Update Risk Assessments

- Evaluate whether your current risk assessment framework adequately addresses the typologies and red flags highlighted in the article.
- Pay particular attention to emerging trends such as use of virtual assets, non-profit organizations, or trade-based money laundering.

2. Enhance Transaction Monitoring & Screening

- Ensure monitoring systems are calibrated to detect patterns aligned with the methods outlined in the article.
- Consider revisiting thresholds and escalation procedures for potentially suspicious transactions.
- Screening customers using sanctions tools such as the Office of Financial Sanctions Implementation Search or similar tool is a crucial process for regulated entities to ensure compliance with regulatory requirements and mitigate the risks associated with engaging with sanctioned entities.

3. Strengthen Customer Due Diligence (CDD)

- Reassess your onboarding processes, especially for high-risk customers or sectors vulnerable to terrorist financing abuse.
- Ensure enhanced due diligence (EDD) measures are in place where required by law.

4. Staff Training and Awareness

- Incorporate key learnings from the article into ongoing AML/CFT training programs.
- Conduct targeted sessions for front-line staff, compliance officers, and senior management on identifying and reporting terrorist financing.

5. Review and Report Suspicious Activity

- Remind staff of the obligation to file Suspicious Transaction Reports (STRs) when terrorist financing is suspected.
- Ensure procedures are in place to escalate concerns quickly and securely to the appropriate regulatory or law enforcement body.

6. Engage with Regulators and Industry Groups

- Stay connected with our latest guidance on counter-terrorist financing (CTF) measures.
- Consider participating in industry forums to stay current on evolving threats.

The threat of terrorist financing is dynamic, and regulated entities must be proactive in adapting their compliance frameworks accordingly. By taking the above steps, regulated entities can not only meet their regulatory obligations, but also contribute to broader national and global security efforts.

Contact Us

For further information, visit our Website at www.tcifsc.tc
Email us at aml_supervision@tcifsc.tc
Email us at amloutreachunit@tcifsc.tc