**FORUM:** General Assembly 5

**QUESTION OF:** Measures to combat the financing of international terrorism

**SUBMITTED BY:** Sweden

**CO-SUBMITTERS:** Guatemala, Antigua and Barbuda, Papua New Guinea, Marshall Islands, The Republic of Cape Verde, Gambia, Vanuatu, Tonga, Tuvalu, Jordan, Tunisia, Czech Republic, Natharlands, Iran Siorra Lagra, San Toma and Britaina, Dominioan Banublic, Natura, Guinea, Grand

Netherlands, Iran, Sierra Leone, Sao Tome and Principe, Dominican Republic, Nauru, Guinea, Greece,

Ecuador, Indonesia, Trinidad & Tobago, Côte d'Ivoire

## FORUM/COMMITTEE: GENERAL ASSEMBLY 5,

*Fully aware* that in 2017 18,800 deaths were associated with global terrorism, and that the Islamic State, the Taliban, Boko Haram, and Al-Shabaab are responsible for the majority of these deaths,

Deeply conscious that religion, globalization, cultural differences, and personal reasons are the main causes of terrorism,

*Noting with deep concern* that the main sources of terrorist funding include charities, fraud, drug trafficking, and legitimate sources,

Expressing its appreciation for the 4th Anti-Money Laundering (AML) Directive introduced by the European Union as well as the Bank Secrecy Act, used to ensure that both customers due diligence and transaction records be retained in compliance with GDPR regulations,

- 1. <u>Encourages</u> all MEDCs to provide aid and resources to LEDCs which would benefit from implementing Anti-Money Laundering (AML) laws but are unable to due to lack of resources and funding which would include:
  - a) identifying states' ability to implement AML measures based on the Basel AML Index
  - b) donating technology that can be used to track money laundering activities, in order to make it easier to track large transactions
  - c) training and skills development focussing on the process, tools, and data management
  - d) offering support to complete audit cycles for AML on a strategic, tactical, and operational level, and delivering recommendations for further enhancement of AML compliance
  - e) supporting in addressing challenges related to implementing
  - f) providing funding from the UN to digitise systems in organizations such as but not limited to:
    - i. banks
    - ii. major companies
    - iii. trade markets:
- 2. <u>Calls upon regional tax examiners/collectors/officials and those who hold similar positions to:</u>
  - a) report unusual transactions to law enforcement or other relevant authorities if an individual is suspected of being a financier based on but not limited to the following criteria:
    - i. the transaction's origins or identity of the involved parties are not recognized by the financial institution's archives
    - ii. the transaction does not fit the sender/receiver's background or reported income
    - iii. there is a sudden shift in currency or to less transparent financial instruments
    - iv. flows to conflict zones or neighbouring regions are present under the name of aid
    - v. funds are entirely or mostly collected from charity and/or non-profit organizations in ways such as anonymous donations
    - vi. use of a letterbox company
  - b) report unusual transactions to law enforcement or other relevant authorities if an individual is suspected of being an organizer in a terrorist organization based on the criteria that:
    - i. rapid transfers of funds following cash deposits are present
    - ii. real estate transactions funded by unknown sources are present

- iii. payment for traveling to a conflict zone or surrounding areas
- iv. buying or selling high-value goods from conflict zones
- c) use their financial expertise and the information held by their department to:
  - i. analyze the transactions of suspected individuals and identify possible locations, supporters and co-conspirators
  - ii. compare transactions of an individual's transactions during and after a terrorist attack to their earlier transactions
  - iii. utilize pre-existing organizations for tax purposes to exchange information with other international departments
- d) cooperate with the United Nations GPML;
- 3. <u>Encourages</u> all member states' regional governments to establish an executive board of experts in tracking money laundering, these boards should:
  - a) have its experts checked by the UNODC, FATF and Transparency International based on their background, where experts will not be appointed unless the aforementioned organizations find that:
    - i. the official is not and will not be corrupt
    - ii. their experience is relevant
    - iii. they are not appointed because of nepotism or other biases in their respective government
  - b) ensure that given regulations are followed
  - c) report cases of unmet guidelines to UN central offices
  - d) work closely with businesses and third-party organizations involved in online banking transactions of large amounts of money in the form of undercover inspection
  - e) introduce departments, which monitor suspicious actions in their national banks in order to prevent money laundering and the resulting funding of terrorism;
- 4. <u>Calls upon</u> governments to hold financial institutions accountable for all terrorist funding moving through them, and recommends nations require these institutions to:
  - implement modern transaction monitoring software on all online transfers, which facilitates rules designed to flag activity based on certain risk factors, such as changes in transaction frequency or volume across customers
  - b) keep records of transactions they deem suspicious for at least 5 years, if that is in order with their countries' laws
  - c) build a comprehensive customer risk profile for flagged individuals which would:
    - i. contain high-quality data about the individual and their spending habits; including name, bank account, address, and social security number
    - ii. audit relatives and close associates, seeing as they may be working with the flagged individual
    - iii. continuously monitor for changes in a customer's risk status over time
  - d) establish automated Anti-Money Laundering monitoring in all nations, which uses machine learning to detect money laundering and contact governments directly with its findings
  - e) read and abide by the Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors;
- 5. <u>Urges</u> member states to criminalise the funding of terrorism under recommendation five of the International Convention for the Suppression of the Financing of Terrorism, and to:
  - a) take legal measures against any individual who:
    - i. raises, receives or provides funds for the purpose of terrorism
    - ii. holds or uses funds for the purposes of terrorism
    - iii. becomes involved in an arrangement to make funds available for the purposes of terrorism
    - iv. facilitates the laundering of terrorist money
  - b) raise awareness on the issue of money laundering and ways to minimize its impact on the

economy through methods such as:

- i. workshops on safe online transactions
- ii. personalized help guides to newly founded companies
- allow law enforcement to have access to banking records, in case of a legal suspicion;
- 6. <u>Suggests</u> the foundation of an international online information and intelligence sharing tool on focused on the issue of international terrorism funding, which would:
  - a) have to abide by international and national law in the course of sharing the information
  - b) have the information shared based on the Common Reporting Standard (CRS) and the recommendations of the Global Forum on Transparency and Exchange of Information for Tax Purposes
  - c) be led and funded by the UN and the UNODC
  - d) be unique for each region to facilitate regional cooperation
  - e) internationally standardized methods used in order to improve LEDCs possibilities
  - f) aim to improve the less developed countries' ability in regards to combatting the financing of international terrorism
  - g) allow for the communication of relevant and needed information between international institutions;
- 7. <u>Further Encourages</u> law enforcement and investigative agencies to improve their activity on issues of terrorism financing and money laundering by:
  - a) starting parallel financial investigations with criminal ones if the crime at hand is a financial one
  - b) ensuring that the relevant law enforcement have the authority of:
    - i. tracing the criminals' actions
    - ii. seizing property that is or might become proceeds of crime
    - iii. freezing assets that were found to be related to the crime at hand
  - c) focusing on interdisciplinary investigations where law enforcement would have access to:
    - i. relevant financial personnel
    - ii. data and intelligence held by banks or other financial institutions such as casinos
    - iii. financial investigation units of their respective countries, while also using their data mining expertise for recognizing criminals
    - iv. regional anti-money laundering institutions that are linked to FATF
    - v. other powers granted by court and other legal entities in the case of a financial crime
  - d) training investigator counterparts where possible on the specific issues of terrorism financing and money laundering;
- 8. <u>Consider</u> the potential use of financial intelligence in order to control and observe Cross-Border Terrorist Financing (TF) risks through:
  - a) appeals to stay actively seized on this matter by controlling:
    - i. suspicious transaction reports, based on national and FATF recommendations and regulations
    - ii. cross-border wire transferring
    - iii. inflows/outflows of assigned funds on a certain matter
    - iv. establish ongoing engagement with foreign correspondances that have previously been recognized as regular contact points regarding this issue.
  - b) maintaining a threshold of low value/limited funding;
- 9. <u>Encourages</u> combating cryptocurrency usage by terrorists through by:
  - a) focusing on identifying suspected individuals' IP (Internet Protocol) addresses through:
    - i. co-operating with exit node operators to receive information regarding individuals suspected of funding terrorism
    - ii. making sure compromised centralized cryptocurrencies are shut down as they

would cause risks to users and allow suspicious activity occur without the authorities' knowledge

- b) operating only on individuals that officers have search warrants against to protect:
  - i. civil liberties
  - ii. personal rights
  - iii. privacy
- c) blockchain transaction analysis and downloading blockchain data using core software;
- 10. <u>Endorses</u> that nations recognise charities and NGOs are responsible for providing a significant portion of funding to international terrorism, and recommends that nations:
  - a) inspect charities and NGOs regularly to ensure that they are not sending money or resources to terrorist organizations, especially groups which have many international bank transactions
  - b) hold trustees of charities responsible for all misconduct taking place, and recommends that the trustees ensure the charities transactions are as transparent as possible
  - c) promoting these organizations to release annual financial statements by:
    - i. by providing tax benefits or deductions from non-profit fees, which would be determined by the respective governments
    - ii. having similar financial requirements to join trade organizations or co-operations between multiple entities;
- 11. <u>Decides</u> to remain actively seized on the matter.