



CAYMAN ISLANDS

Registrar of Non-Profit Organizations

## **Guidance: Best Practices to prevent a Non-Profit Organisation from being Abused for Terrorist Purposes**

Version Number: 1.0  
Date of Version: 08 January 2020  
Creator: Cayman Islands General Registry, Compliance Unit  
Approver: Cindy Jefferson-Bulgin

Date Approved:  
Confidential Level: Low



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

**TABLE OF CONTENTS**

<b>1. INTRODUCTION</b> .....	2
<b>2. NPOS AND TERRORISM</b> .....	2
<b>3. THE TERRORISM LAW</b> .....	3
<b>4. STAGES OF TERRORIST FINANCING</b> .....	5
4.2. Raise .....	5
4.3. Store .....	5
4.4. Move .....	5
4.5. Use .....	5
<b>5. VULNERABILITIES</b> .....	6
<b>6. NPO SECTOR OPERATIONS AND VULNERABILITIES</b> .....	8
<b>7. EXAMPLES OF TECHNIQUES USED TO ABUSE NPOS</b> .....	8
7.2. Abuse by Internal Parties .....	8
7.3. Abuse by External Parties through the Use of NPOs’ Assets or Purpose .....	9
7.4. NPOs Established for Illegal or Improper Purposes .....	10
7.5. Cyber-terrorism.....	10
<b>8. INTERNAL CONTROLS THAT AID IN MITIGATING THE FINANCING OF TERRORISM</b> .....	11
8.2.1. Governance .....	11
8.2.2. Record Keeping.....	11
8.2.3. Bank Account .....	12
8.2.4. Cash Collection Protocols .....	12
8.2.5. Use of Cash or Resources .....	12
8.2.6. Know Your Benefactor .....	13
8.2.7. Use of Intermediaries of Reputable Third Parties .....	13
8.2.8. Use of Search Engines .....	13
<b>9. MANAGEMENT OF RISK AND RISK ASSESSMENT OF NPOS</b> .....	13
<b>10. REPORTING SUSPICIOUS ACTIVITY</b> .....	15



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

**1. INTRODUCTION**

- 1.1. The National Terrorist Financing Risk Assessment (2019) concludes that there is a very low risk of terrorist acts occurring in the Cayman Islands or citizens of the Cayman Islands committing acts of terrorism. Similarly, the Cayman Islands Non-Profit Organizations (“NPOs”) Risk Assessment (2019) indicates that the risk of terrorist financing in the NPO sector is low but not impossible.
- 1.2. The purpose of this guidance, which serves as a reference/education tool for NPOs to combat and mitigate terrorist financing preventatively, is to:
  - 1.2.1. address vulnerabilities associated with NPOs being abused for direct terrorist financing or indirect facilitation of a terrorist act;
  - 1.2.2. further raise awareness of key counter-terrorism legislation in the Cayman Islands; and
  - 1.2.3. provide guidance in developing sound internal risk measures, governance, strategies, policies, procedures, and other internal controls.

**2. NPOS AND TERRORISM**

- 2.1. The NPO sector in the Cayman Islands is diverse, multi-cultural, and far-reaching, spanning many different types, sizes, objectives, and activities. However, the common denominator of all NPOs is the unified commitment to voluntary action, with a desire to improve living standards and quality of life. For instance, whilst many NPOs tackle potential causes of alienation in communities, some concentrate on promoting and upholding human rights and others provide aid or supply essential services.
- 2.2. Generally, the integral output of the NPO sector positively impacts domestic and international communities, significantly influencing macroeconomic issues such as crime, unemployment, inflation, and economic growth. NPOs tend to work in impoverished areas, sometimes delivering in adverse and extreme conditions, which often complements the arbiter of society’s (i.e. Government’s) aim to maximize social welfare insofar as possible. Given the nature of their work, NPOs usually establish trusting relationships with the public and are, at times, more comprehensively aware of local issues than public or private bodies. Therefore, it is vital that governments maintain an open dialogue with the NPO sector to build a culture where NPOs are comfortable sharing intelligence of illegalities and other matters against the public interest.



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

2.3. The financial sector of the Cayman Islands' economy has continuously tightened safeguards and defenses against terrorism. As vulnerabilities in the financial sector are effectively addressed, terrorists and other criminal agents will likely attempt to exploit sectors and industries with loopholes, technical weaknesses, and corruption and/or sectors and industries subject to light touch regulation.

**3. THE TERRORISM LAW**

3.1. Many NPOs, like other parts of society, condemn terrorist acts and carry out much work to alleviate conditions that may lead people to participate in extremism or terrorism. The Cayman Islands Terrorism Law (2018 Revision) ("TL") criminalized terrorism and terrorist financing. The TL defines several important terms as tabled below.

Term	Definition	Section of TL
3.1.1. <b>Terrorism</b>	(a) An act whether committed in or outside of the Cayman Islands which causes or is likely to cause: i. loss of human life or serious bodily harm; ii. damage to property; or iii. prejudice to national security or disruption of public safety including disruption in the provision of emergency services or to any computer or electronic system or to the provision of services directly related to banking, communications, infrastructure, financial services, public utilities, transportation, or other essential infrastructure, and is intended to: A. compel a government or an international organization to do or refrain from doing any act; or B. intimidate the public or a section of the public,	Part I



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

Term	Definition	Section of TL
	for the purpose of advancing a political, religious, racial, or ideological cause; or  (b) An offence under sections 3 to 7, 14 to 16, and 19 to 22.	
3.1.2. <b><i>Terrorist Property</i></b>	Property that is the proceeds of, or used in, or intended or allocated for use in, the financing of acts of terrorism, terrorists, or terrorist organizations.	Section 18
3.2.3 <b><i>Use and Possession of Terrorist Property</i></b>	A person commits an offence if that person uses property for the purposes of terrorism. A person commits an offence if that person:  (a) possesses terrorist property and intends that it should be used, or has reasonable cause to suspect that it may be used, for the purpose of the financing of acts of terrorism, terrorist or terrorist organizations;  (b) Possesses or acquires terrorist property which the person knows or has reasonable cause to suspect has been used, directly or indirectly, in the commission of the financing of acts of terrorism, terrorists or terrorist organizations; or  (c) Acquires property as a result of, or in connection with acts of terrorism.	Section 20

3.2. The TL also includes information with respect to the following subject matters and the corresponding sections have been bracketed for ease of reference:

- 3.2.1. substantive terrorism offences (sections 3-17);
- 3.2.2. life imprisonment for terrorism offences (section 3);
- 3.2.3. weapons training sentence of 6 months in summary court or 10 years on indictment (section 4);
- 3.2.4. use of certain weapons (sections 5, 6, and 7);



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

- 3.2.5. defenses to offences under sections 4-7 where there is an absence of reasons to believe the object was for terrorism purposes (section 9);
- 3.2.6. extra-territorial power to the Cayman Islands to prosecute offences (section 10);
- 3.2.7. a company may be prosecuted for substantive offences (section 12);
- 3.2.8. possession of article for terrorist purposes (section 15);
- 3.2.9. inciting, organizing, and travelling for terrorism (section 16);
- 3.2.10. duty to disclose information relating to offences and terrorist acts (section 17); and
- 3.2.11. the offence of possessing or treating with terrorist property (sections 18-22).

#### **4. STAGES OF TERRORIST FINANCING**

4.1. The process of terrorist financing is comprised of four stages: raise, store, move, and use.

##### **Raise**

4.2.1. NPOs raise funds through various means, depending on its purpose and activities, such as donor solicitation. The abuse of the NPO at this stage can occur through the diversion of funds raised by an internal individual, or third party, or by the NPO itself having been deliberately and illegitimately established for terrorist financing purposes.

##### **Store**

4.3.1. Money or resources (for example humanitarian aid) is stored in a legitimate financial institution, at the NPO's physical address, or at another designated location.

##### **Move**

4.4.1. NPOs move money or resources through various methods depending on the nature and type of NPO, although all NPOs in the Cayman Islands are required to move money via a domestic retail bank. On the other hand, resources are usually moved through import and export via a legitimate shipping company.

4.4.2. At this stage, assuming that the NPO is involved in terrorist financing (directly or indirectly), at some point, money or resources are likely moved using an illegal means such as scamming or fraud.

##### **Use**

4.5.1. NPOs use money to cover various operational costs including rent, utilities, salaries, propaganda and recruitment, training as well as social services.



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

- 4.5.2. This stage presents the greatest risk for camouflaging terrorist financing as terrorists and terrorist organisations use money to settle costs which are similar (and often identical) to costs arising from legitimate NPO activity.
- 4.5.3. It is imperative that NPOs fully understand their operations, including delivery channels and distributions, as well as the weaknesses and threats that are present or may potentially materialize.. Having conducting such an analysis, the governing body and management of the NPO are required to abate any risks through selective mitigative measures (as indicated in the risk management guidance).

## **5. VULNERABILITIES**

- 5.1. International guidance on terrorism suggests that the recent threats posed by international terrorism are different in nature and scale to terrorist threats faced in the past. International terrorism is motivated by an extremist ideology and exploits modern travel and communications in order to spread through global networks. Terrorism is ever-evolving as terrorists continuously develop new methods and take advantage of new technologies.
- 5.2. Published international non-fictional typologies and case studies have proven that terrorists and terrorist organizations abuse the NPO sector to raise, store, move, and use funds as well as provide logistical network support, recruit, and otherwise support terrorist operations.
- 5.3. As per the risk assessment conducted by the Registrar of NPOs, the NPO sector in the Cayman Islands has never been penetrated for terrorist purposes. Nonetheless, the NPO sector has vulnerabilities that, if left unchecked, can be potentially exploited for terrorist and other criminal purposes. Vulnerabilities exist because NPOs:
- 5.3.1. enjoy high levels of public trust and confidence, which is crucial to their success;
  - 5.3.2. often rely on goodwill and voluntary support in one form or another;
  - 5.3.3. are diverse in nature and activities, often connecting to all parts of society and various high risk jurisdictions; due to this connectivity, a large number of persons come into close contact with NPOs, including those who may abuse them, through their services, property, staff, and volunteers;
  - 5.3.4. are easy to legally set up;
  - 5.3.5. may depend on one or two individuals who play a key, and often unsupervised, role, which is particularly the case with smaller NPOs;
  - 5.3.6. have a global presence, including in conflict areas and/or where there is little infrastructure, and frequently move money, goods, and people to these areas;



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

- 5.3.7. sometimes have complex financial operations encompassing multiple donors, investments, and currencies;
  - 5.3.8. can be heavily cash intensive, in terms of income and expenses, and are accustomed to justifying high volumes of small scale transactions and using remittance transfer services;
  - 5.3.9. may have complex programs of operation, channeling funds through intermediate partner organisations to deliver services; as well as operating directly themselves
  - 5.3.10. may have unpredictable and unusual income and expenditure streams, therefore suspicious transactions may be harder to identify;
  - 5.3.11. may have branches and/or projects that are not under the direct supervision or regular control of management; this is particularly concerning where there is poor governance as well as accurate and regular reporting;
  - 5.3.12. may be internationally subject to different, and in some cases non-equivalent, levels of regulation than in the Cayman Islands; and
  - 5.3.13. are powerful and effective vehicles for connecting people together for a common purpose and collective action, which may inadvertently provide a ready-made social network and platform to give a veneer of legitimacy to terrorism.
- 5.4. The abuse of NPOs for terrorist purposes may take a variety of different forms, especially given the diverse nature of the sector, delivery channels, products, services, and jurisdictions of operation. The NPO's funds, facilities, and name are precious assets which can be exploited for terrorist purposes. History shows that these assets are usually at greater risk from influences outside of the NPO, although abuse can also happen from within the NPO or be carried out by a connected party.
- 5.5. Terrorists seeking to abuse NPOs may view them as a vulnerable target because of the high level of public trust and confidence there is in the NPO sector. Such individuals may abuse NPOs by way of unauthorized use of a NPO's trade name, as well as intercepting and redirecting international operations, which likely involve access to vulnerable or restricted communities and their financial system.
- 5.6. While the risks of abuse may increase where a NPO operates in, or has connections to, unstable or high risk countries, the risk of abuse are also applicable to NPOs operating in the Cayman Islands.





CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

**6. NPO SECTOR OPERATIONS AND VULNERABILITIES**

6.1. A NPO's system/network of operations can be categorized, as tabled below, and there are inherent vulnerabilities associated with each phase which may decrease or increase depending on the type of NPO, as well as the NPO's size, purpose and activities, delivery channels, and complexity of operations.

Phase	Definition
<b>Collection</b>	Any activity undertaken by an NPO to increase monetary and non-monetary resources, either directly or indirectly through third parties such as volunteers;
<b>Retention</b>	The storage or maintenance of resources by an NPO, ranging from the maintenance of funds within a bank account to the management of property or facilities.
<b>Transfer</b>	The movement of any resources, which can occur at any point during the NPO's operations, domestically or internationally, to and/or from any economic agent.
<b>Expenditure</b>	The NPO's purchase of any economic good and/or service in exchange for legal tender and/or a bartered object and/or service.
<b>Delivery</b>	The transport and/or distribution of money, goods, and/or service, especially where programs have been established.

**7. EXAMPLES OF TECHNIQUES USED TO ABUSE NPOS**

7.1. Noteworthy, irrespective of the technique used, the abuse of NPOs is usually initiated with a fraudulent activity including, but not limited to, forgery of signatures, falsifying (and unauthorized manipulation of) documents (i.e. receipts, invoices, emails, and financial statements), deliberate misrepresentation of facts, and Ponzi like schemes, therein lies the need for effective internal controls, especially those of a preventative nature.

**7.2. Abuse by Internal Parties**

7.2.1. Individuals, such as Controllers and volunteers, appointed within a NPO in some capacity may abuse their position in order to contribute to terrorist activity, oftentimes in exchange for a monetary or non-monetary benefit.

7.2.2. Abuse of power and position to facilitate terrorist activity (directly or indirectly) may take place via:

7.2.2.1. 'skimming' off/stealing money, or other assets, from charitable collections and redirecting;



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

- 7.2.2.2. arranging for the use of the NPO's premises; and
- 7.2.2.3. deliberately inviting speakers or using volunteers with terrorist motives to visit and work with the NPO in order to influence the NPO's operations in such a way that supports terrorist activity.

7.3. **Abuse by External Parties through the Use of NPOs' Assets or Purpose**

7.3.1. Individuals supporting terrorist activity may claim to work for a NPO and trade in its reputable name in order to gain access or travel to a particular region or community for propagation or training purposes.

7.3.2. A NPO's:

- 7.3.2.1. uniform may be stolen and used to present the notion that funds are being raised for and on behalf of the NPO; however, in fact, those funds and resources are being diverted for terrorist purposes. Where a NPO's funds are being moved from one place to another, including internationally, they could be diverted before reaching their intended recipients; a NPO might be used to launder money, acting as a front for placing, layering, or integrating money or other financial instruments. This risk is particularly high where the NPO's financial controls are weak and thus, it is vital that every stage in the workflow is tested at the onset and periodically thereafter;
- 7.3.2.2. vehicle may be stolen and used to transport or smuggle people, cash, weapons, terrorist propaganda, drugs, and other illicit and contraband good. Similarly, a NPOs' premises may be commandeered to facilitate storage and distribution for terrorist purposes;
- 7.3.2.3. communications network could be exploited to allow terrorists to make contact and/or arrange meetings without the NPO's (or Controllers') knowledge. Those NPOs which participate in in missionary work and sponsorship of humanitarian aid must be aware of such vulnerabilities and have the requisite controls in place to prevent, detect, and correct said vulnerabilities; and
- 7.3.2.4. resources may be used to support the basic economic needs of a Foreign Terrorist Fighter's ("FTF's") family while the FTF is away. Where a NPO has been established to provide essential support aid to the public, yet chooses



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

to provide relief only to the families of terrorists or a particular terrorist organization, this is not legitimate activity; although the family of a FTF may genuinely be in need, the unstated and underlying purpose of the NPO becomes to help the FTF or terrorist organization carry out terrorist activities.

7.3.3. Terrorist activities may be hidden or camouflaged by or take place alongside normal and otherwise legitimate, charitable activities. A NPO may give financial or other support to an organisation or partner that provides legitimate aid and relief. However, that organisation or partner may also support or carry out terrorist activities. Therefore, the onus is on the NPO to carrying out comprehensive vetting prior to forming relationships with said organizations and partners. For instance, a school that teaches terrorist ideology, or trains terrorist recruits, alongside proper classes in areas like information technology may be able to provide full receipts demonstrating the use of the NPO's funds to purchase necessary goods and services.

7.4. NPOs Established for Illegal or Improper Purposes

7.4.1. In extreme cases, terrorists may attempt to set up an organisation as a sham, promoting it as charitable with the sole intended purpose to raise funds or use its facilities or name to promote or coordinate inappropriate and unlawful activities. It is important to remember that there is no indication that any of the NPOs registered in the Cayman Islands to date have been set up for terrorist purposes or are involved in the financing of terrorism; the risk of terrorism and financing of terrorism in the NPO sector remains low. Nevertheless, care should always to taken to verify the legitimacy of a NPO before providing donations or volunteering to serve.

7.5. Cyber-terrorism

7.5.1. Cyber-terrorism refers to the ideologically motivated misuse of computers and information technology to cause severe disruption, widespread fear, destruction, and/or harm in support of a group's aims and objectives.

7.5.2. All NPOs use the internet in one form or another, either for collection or dissemination of information and/or documentation. NPOs have been abused through various methods of cyber-crime including crowd funding, spoofing, and phishing emails. Through these methods, NPOs are duped into providing funding or resources either to terrorist organisations or criminal networks that support terrorism. Controllers and Senior Officers must exhibit care and diligence at all times when using the internet,



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

which includes: never providing passwords or account information, clicking or downloading links without preliminary knowledge of the contents, and utilizing virus protection. NPOs conducting wire transfers should, as a best practice, establish a second tier control with the financial institution as a way to ensure that all messages to move money are legitimate in nature; simple measures like a call back can serve as a good additional control to avoid the approval of fraudulent wire instructions.

**8. INTERNAL CONTROLS THAT AID IN MITIGATING THE FINANCING OF TERRORISM**

8.1. NPOs registered in the Cayman Islands are required to implement internal controls which mitigate the risk of terrorist financing. As there is no one size fits all approach to internal controls, NPOs are required to understand its specific terrorist financing risk and implement tailored risk management measures.

8.2. Generally, at minimum, the Registrar of NPOs expects the following to be in place.

8.2.1. **Governance**

8.2.1.1. Regular Board or Management Committee meetings must be held in order to make organizational decisions, particularly those related to income and expenditure. All meetings must be recorded by way of documented and executed minutes, which should be maintained on file as part of the NPO's record retention policy;

8.2.2. **Record Keeping**

8.2.2.1. NPOs must have a documented record retention policy, duly approved by the governing body, which outlines the:

8.2.2.1.1. type of records (for instance, financial statements, minutes, receipts, donation sheets, client due diligence documents, et cetera) to be maintained and the corresponding retention periods; records relating to ongoing litigations and investigation must be maintained for a period of five years or until the litigation and investigation is concluded, whichever is greater; equally, client due diligence documents (i.e. passports, information obtained from the internet, et cetera) should be maintained for the duration of a particular relationship;



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

8.2.2.1.2. conditions in which records must be kept; all records, which should be legible, in English, up to date, and certified where appropriate, must be easily accessible; and

8.2.2.1.3. record management system used, whether electronic or non-electronic.

**8.2.3. Bank Account**

8.2.3.1. NPOs are required to establish a bank account with a regulated domestic retail bank in the Cayman Islands in order to carry out all domestic and international transactions.

8.2.3.2. Where money is being collected or sent via a regulated money service business (for instance JN Money Transfer) caution must be exercised to ensure that the NPO knows the sender or recipient from a client due diligence perspective. In such cases, the NPO should provide the money service business with all relevant details and maintain copies of all receipts.

**8.2.4. Cash Collection Protocols**

8.2.4.1. NPOs are required to have in place protocols or measures that circumvent and mitigate theft or abuse of assets. Basic measures should include segregation of duties, that is, there should be a separation between persons who collect, count/reconcile, and deposit the money.

**8.2.5. Use of Cash or Resources**

8.2.5.1. NPOs should require dual signatures to any account, whether chequing, savings, or investments, and establish a reasonable threshold above which prior authorization from the Board/Management Committee is mandatory. For example, any expenses above a CI\$1000.00 must be authorized by the Board/Management Committee in writing.

8.2.5.2. NPOs should collect and maintain appropriate client due diligence documents for all account signatories, who must be connected to the NPO in some capacity. Changes to account signatories should be approved in writing by the governing body.



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

**8.2.6. Know Your Benefactor**

8.2.6.1. NPOs must have documented processes in place that allows it to reasonably know (where applicable) beneficiaries of funds (and other resources) as well as obtain evidence for the intended use thereof.

**8.2.7. Use of Intermediaries of Reputable Third Parties**

8.2.7.1. NPOs involved in sending funds or aid to international jurisdictions, particularly high risk jurisdictions, should consider acquiring the services of a reputable and experienced third party which already has a physical presence in the recipient jurisdiction. The NPO must have documented procedures in place for vetting such third parties.

**8.2.8. Use of Search Engines**

8.2.8.1. NPOs should utilize credible sources/websites to conduct basic due diligence on individuals or entities prior to sending funds or aid. For example, the United Nations' website has a free search function where checks can be made to ensure that proposed beneficiaries are not designated persons or entities.

**8.2.9. Training**

8.2.9.1. The Registrar of NPOs will be providing ongoing training and sensitizing sessions for the NPO sector on the risk of terrorist financing, targeted financial sanctions and countering proliferation financial sanctions. These sessions will comprise both face to face sessions and online training via General Registry's website. As a best practice, NPOs should also consider internal training within their respective organisations. The Registrar where applicable can assist with such sessions.

8.3. All policies and procedures must be approved by the governing body and updated when required.

**9. MANAGEMENT OF RISK AND RISK ASSESSMENT OF NPOS**

9.1. Section 4 of the NPO Law (2017) mandates that the Registrar of NPOs ensure that NPOs have appropriate internal controls in place to reduce the risk of terrorist financing.

9.2. Amongst other requirements, NPOs are required to:



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

- 9.2.1. implement internal controls, inclusive of a solid governance framework and procedure for maintaining financial statements for a minimum of five years;
  - 9.2.2. have a sound understanding of their purpose and activities, as well as the location of activities and method of how activities will be carried out, and apply risk based approach to rectify any current or potential vulnerabilities;
  - 9.2.3. employ risk management practices that range from formal policies and procedures, which outline internal practices and procedures, duly regarding sound best practices and accounting principles; and
  - 9.2.4. implement simple internal rules with respect to, for example, matters relating to segregation of duties. It is essential that each NPO conduct an internal assessment of its processes, giving consideration to safeguarding the solicitation, collection, and dispersal of funds. This assessment should also take into consideration management oversight, approvals, and record keeping.
- 9.3. For smaller NPOs, controls must include dual signatures on the NPO's bank accounts. In addition, the Board of Directors (or Committee) should grant authorizations, accompanied by written executed copies of the related minutes and/or resolutions, prior to the disbursement and dissemination of money and/or other resources valuing CI\$500.00 or greater.
- 9.4. For larger and more established NPOs, there is an expectation that the Directors comply with the standards established by the Companies Law (2018) and other relevant legislation used in the financial services industry. Internal controls must be commensurate with its scale and complexity.
- 9.5. For a more granular explanation of internal controls, please refer to "Best Practices for the NPO Sector", which is available on the General Registry's website.
- 9.6. To address the issue of cyber-crime risk, controllers, senior officers, and other staff members of NPOs are encouraged to use caution and apply enhance due diligence when providing financial support or banking details online. The golden principle, "you cannot win what you've never played". It is recommended that NPOs not respond to or communicate with unknown persons online without verification and remember that financial institutions in the Cayman



CAYMAN ISLANDS  
Registrar of Non-Profit Organizations

Islands do not request personal or account details online. When in doubt always call the financial institution in question.

**10. REPORTING SUSPICIOUS ACTIVITY**

- 10.1. Attention is drawn to sections 12 and 17 of the TL with respect to offences by a body corporate and a duty to disclose information relating to terrorist acts.
  
- 10.2. Where you suspect that any of the aforementioned red flags apply to any NPO registered in the Cayman Islands, you have a legal obligation to report all relevant information to the Registrar of NPOs and Royal Cayman Islands Police Service. Please refer to “Guidance on Reporting a Complaint on a NPO”, which is located on the General Registry’s website.