

KNOW YOUR CUSTOMER QUESTIONNAIRE

Section A - Details

A1. Legal Form, Regulatory status and Other Details

1.1 What is the legal form of your institution?	
<input type="checkbox"/> Public company	<input checked="" type="checkbox"/> Private company
<input type="checkbox"/> State Owned Company	
<input type="checkbox"/> Other (please provide full details):	
1.2 Is your Institution Regulated?	
Does your Institution have a supervisory authority such as a government agency that is responsible for AML/CFT monitoring in your jurisdiction?	<input checked="" type="checkbox"/> Yes - Name the regulator(s) below: Central Bank of Trinidad and Tobago www.central-bank.org.tt <input type="checkbox"/> No

1.3 Is your institution or parent institution a publicly traded entity?	
<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
If yes, please list the Stock Exchange (s) and stock symbol : RFHL	
Where applicable, name of parent company: Republic Financial Holdings Limited	

1.4 AML/CFT Audit Details	
Date of last internal audit:	
Is your Institution audited externally?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
If so, by whom: Ernst & Young	
Date of last external audit: October 30 2019	

A2. Ownership

2.1 Specify below all owners, significant/controlling shareholders of your Institution (including beneficial owners of shares that are not natural persons (e.g. companies, foundations, trusts etc.) i.e.:

- Those persons holding more than 10% of the available voting rights in the company.
- Any other person/ shareholder that exerts significant influence / control over the business (regardless of size of interest)

Name	Address of each person/entity	Size of interest	Comments
Republic Financial Holdings Limited	9-17 Park Street Port of Spain Trinidad and Tobago	100%	

2.2 Is any part of the organisation state owned?:

If yes, please provide details of ownership and shareholding:

A3. Anti Money Laundering (AML) Controls and Assessment

I. General AML Policies, Practices and Procedures:

1. Is the FI fully compliant with the Anti Money Laundering / Terrorist Financing laws in your country?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
2. Is the AML compliance program approved by the FI's board or a senior committee?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
3. Does the FI have a legal and regulatory compliance program that includes a designated officer that is responsible for coordinating and overseeing the AML framework?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
4. Has the FI developed written policies, controls and procedures designed to prevent, detect and report suspicious transactions?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
5. Does the FI have a policy prohibiting accounts/relationships with shell banks? (A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.)	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
6. Does the FI have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
7. Does the FI have policies regarding accounts for MSBs and PMCs/Casinos?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
8. Does the FI have policies covering relationships with Politically Exposed Persons (PEP's) ¹ , their family and close associates?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
9. Does the FI have record retention procedures that comply with applicable law?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
10. If you have branches or subsidiaries outside of your Head Office Country, are you institution's AML policies and practices being applied to all branches and/or subsidiaries and/or separate legal entities whether they are in the home country or in locations outside of that jurisdiction?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
11. Does the FI offer anonymous accounts, i.e. numbered accounts for which the FI does not have full particulars of the beneficial owner?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
12. Does the FI provide services to non-account customers? (E.g Cashing of cheques, travelers cheques, wire transfer remittance)	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No

If yes, what controls does your organisation have in place to mitigate the risk for non-account customer transactions? Non Account customers can only exchange foreign currency

¹ A Politically Exposed Person (PEP) is a senior local &/or foreign political figure, any member of the PEP's immediate family and any close associate of the PEP. A "senior political figure" is a senior official in the executive, legislative, administrative, military, judicial branches of a government (whether elected or not), a senior official of a major political party, or a senior executive of a government-owned corporation. Any business or other entity that has been formed by, or for the benefit of the PEP's "immediate family" (i.e., parents, siblings, spouse, and children). "Close associate" is a person who is widely and publicly known to maintain an unusually close relationship with the PEP, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the PEP.

KNOW YOUR CUSTOMER QUESTIONNAIRE

To be completed by Listed Businesses; Non-regulated financial institutions (i.e. Building Societies, Co-operative Societies and Money or Value Transfer Service Providers) and Financial Intermediaries (FIs) (e.g. Banks, Mutual Funds, Credit Unions, Life Insurance Companies, Finance Companies)

II. Risk Assessment	
13. Does the entity conduct a risk-based assessment of its customer base and their transactions?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
14. In relation to the entities products, services, transactions and delivery channels ³ , does the entity consider the following attributes: <ul style="list-style-type: none"> • Nature, scale, diversity and complexity of its business activities; • Nature of products and services offered • Nature of delivery channels utilized? 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
15. Does the entity determine the appropriate level of enhanced due diligence necessary for those categories of customers, transactions and delivery channels that the entity has reason to believe pose a heightened risk of illicit activities at or through the entity?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
16. Does the entity conduct a group-wide ML/TF risk assessment at least once in two years or when material trigger events occur, whichever is earlier? <i>Material trigger events include but are not limited to the acquisition of new customer segments or delivery channels or the launch of new products or services.</i>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
III. Know Your Customer, Due Diligence and Enhanced Due Diligence	
17. Has the entity implemented processes for the identification of those customers on whose behalf it maintains or operates accounts or conducts transactions?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
18. Does the entity have a requirement to collect information regarding its customers' business activities?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
19. Does the entity assess its FI customers' AML/CTF policies or practices?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
20. Does the entity have a process to review and, where appropriate, update customer information relating to high risk customers?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
21. Does the entity have procedures to establish a record for each new customer noting their respective identification documents and 'Know Your Customer' information?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
22. Does the entity complete a risk-based assessment to understand the normal and expected transactions of its customers?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
IV. Reportable Transactions and Prevention and Detection of Transactions with Illegally Obtained Funds	
23. Does the entity have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
24. Where cash transaction reporting is mandatory, does the entity have procedures to identify transactions structured to avoid such obligations?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
25. Does the entity screen customers and transactions against lists of persons, entities or countries issued by government/competent authorities?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
26. Does the entity have policies to reasonably ensure that it only does business with correspondent banks that possess licenses to operate in their countries of origin?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
27. Does the entity adhere to the Wolfsberg Transparency Principles and the appropriate usage of the SWIFT MT 202/202COV and MT 205/205COV message formats? ⁴	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
V. Transaction Monitoring	
28. Does the entity have a monitoring program for unusual and potentially suspicious activity that covers funds transfers and monetary instruments such as traveler's checks, money orders, etc?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
29. If the answer to question 28 is yes, does the entity have an automated transaction monitoring system? if no, what controls does your organisation have in place to monitor for unusual and potentially suspicious activity?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
VI. AML Training	
30. Does the entity provide AML/CTF training to relevant employees that includes: <ul style="list-style-type: none"> • Identification and reporting of transactions that must be reported to government authorities • Examples of different forms of money laundering involving the FI's products and services • Internal policies to prevent money laundering. 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
31. Does the entity retain records of its training sessions including attendance records and relevant training materials used?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
32. Does the entity communicate new AML/CTF related laws or changes to existing AML/CTF related policies or practices to relevant employees?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
33. Does the entity employ third parties to carry out some of its functions?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

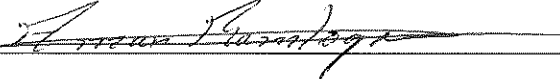
³ Delivery channel in this context is the way means whereby an entity carries on its business relationship with a customer, i.e., directly or through other means such as email, Internet, intermediary, or any correspondent institution.

⁴ The four payment message standards to be observed are: i) FIs should not omit, delete, or alter information in payment messages or orders for the purpose of avoiding detection of that information by any other FI in the payment process; ii) FIs should not use any particular payment message for the purpose of avoiding detection of information by any other FI in the payment process; iii) Subject to applicable laws, FIs should cooperate as fully as practicable with other FIs in the payment process when requesting to provide information about the parties involved; and (iv) FIs should strongly encourage their correspondent banks to observe these principles. Source: [http://www.wolfsbergprinciples.com/pdf/standards/Wolfsberg_NYCH_Statement_on_Payment_Message_Standards_\(2007\).pdf](http://www.wolfsbergprinciples.com/pdf/standards/Wolfsberg_NYCH_Statement_on_Payment_Message_Standards_(2007).pdf)

<p>34. If the answer to to question 33 is yes, does the entity provide AML/ctf training to relevant third parties that includes:</p> <ul style="list-style-type: none"> • Identificatio and reporting of transactions that must be reported to government authorities • Exaples of different form os money laundering involving the entity's products and services • Internal policies to prevent money laudering 	<input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A
VIII. Other	
<p>35. Has your institution been subject to any money laundering /terrorist financing investigations or other regulatory action in your country or in any other country?</p> <p>If yes, please provide details:</p>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Section B – Authorised Signatory:

Attestation Statement : The information completed on this questionnaire is accurate to the best of my knowledge and there are no material omissions.

Name:	Amar Ramlogan
Position:	Manager, Risk Rating and Due Diligence
Address:	72 Independence Square, Port of Spain, Trinidad and Tobago
Telephone:	625-3617
E-mail:	amar.ramlogan@rfhl.com
Signed :	
Date:	06/04/20