AML/CFT/CPF REQUIREMENTS FOR ELECTRONIC MONEY ISSUERS ("EMIs")

INTRODUCTION

EMIs are subject to the joint supervision of the Central Bank of Trinidad and Tobago ("Central Bank") and the Financial Intelligence Unit of Trinidad and Tobago ("FIUTT"). Prudentially, EMIs are regulated and supervised by the Central Bank of Trinidad and Tobago ("Central Bank"), pursuant to the EMI Order, 2020.

Based on the nature of their business activity, EMIs are categorized as Money or Value Transfer Service ("MVTS")[1] providers. Under Section 2 the Proceeds of Crime Act, Chap.11:27 ("POCA"), MVTS providers are included in the definition of a 'financial institution' and are therefore required to comply with AML requirements. Further, as a non-regulated financial institution, EMIs are required to register with the FIUTT[2] and to establish risk-based AML programs approved by senior management[3]. In this regard, in respect of compliance with Anti-Money Laundering/Counter Financing of Terrorism/Counter Proliferation Financing (hereinafter "AML") requirements, EMIs are supervised by the FIUTT.

AML RISK ASSESSMENT

EMIs are required to conduct a money laundering/terrorist financing/proliferation financing (ML/TF/PF) risk assessment of their business operations and establish AML policies and procedures to mitigate the identified risks[4]. The following are some ML/TF risk factors associated with E-Money which the EMI should consider when conducting the risk assessment. This is not an exhaustive list.

- Enables cash funding and withdrawals ("cash-in" and "cash-out" functions);
- Account holder with multiple accounts;
- Use of agents to distribute e-money on behalf of the issuer without appropriate governance and oversight by the issuer; and
- Agents conducting customer due diligence on behalf of the issuer but are not properly trained on the issuer's AML programme.

AML COMPLIANCE PROGRAMME

The EMI is required to designate a Compliance Officer ("CO") in accordance with Regulation 3 of the FORs and seek the approval of the Central Bank and the FIUTT. The CO is responsible for ensuring the EMI's AML Compliance Programme satisfies the AML legislation and regulatory guidelines. A suitable alternate for the Compliance Officer[5] who must be approved by the FIUTT, must also be identified to execute the compliance function in the absence of the CO. The EMI must ensure that the CO and their alternate receive specialized training to enable them to fulfil their obligations under Regulation 4(1) of the FOR.

---

[1] EMIs fall within the category of money and value transfer services ("MVTS") based on activities performed, which satisfy the three (3) basic elements of the definition of MVTS under Regulation 2 of the Financial Obligations Regulations 2010 (as amended) ("FOR"):

a. The acceptance of monetary instruments or stores of value;
b. The payment or settlement of a corresponding value in another location; and
c. Effecting the payment transfer through a network to which the EMI belongs.

[2] See Section 2 of the FIUTT Act, Chap. 72:01 (FIUTTA) in the definition of 'non-regulated financial institution' and Section 18B of the FIUTTA, and Regulation 2 under the definition of 'Supervisory Authority' in the Financial Obligations Regulations, 2010 (as amended)

[3] Senior management means the body responsible for directing and overseeing the performance of the EMI, and where applicable, will be the Board of Directors of the EMI.

[4] See Part III of the AML/CFT Guideline for guidance on conducting an ML/TF risk assessment and the FIU's Guidance to Non-Regulated Financial Institutions and Listed Businesses on how to Structure an AML/CFT Compliance Programme

[5] Refer to Regulation 3(8) of the FOR

The AML Compliance Programme should include the following[6]:

- Risk based internal systems, processes and controls to ensure ongoing compliance with AML requirements, including inter alia processes for conducting customer due diligence and enhanced due diligence, transaction monitoring, screening against lists of designated persons and high risk entities/countries[7]; and for reporting suspicious activities / transactions, terrorist funds and quarterly terrorist property reports to the FIUTT;
- External audits to verify compliance with AML requirements;
- Training of relevant personnel and agents in the identification, monitoring and reporting of suspicious transactions.

RISK BASED CUSTOMER DUE DILIGENCE

The EMI is required to have risk based onboarding policies [***See Appendix I for the minimum KYC thresholds for individuals / SMEs / companies***] which are commensurate with the risk level identified by the EMI, including simplified measures for lower risk clients and enhanced due diligence for higher risk clients. The policies should include:

- Customer identification and verification measures for individual and business customers. The EMI may implement a higher standard than those outlined in Appendix I based on its risk appetite;
- Identification and risk classification of PEPs;
- Identification of designated entities; and
- Identification of suspicious activity.

ONGOING KNOW YOUR CUSTOMER/ CUSTOMER DUE DILIGENCE

EMIs are expected to conduct monitoring of customer activity and transactions on an ongoing basis. Transaction monitoring may not necessarily require sophisticated electronic systems and a review of transaction value and volume reports on an appropriate frequency[8] may be adequate in some instances. We note that automated systems add value as they are more effective for managing larger volumes of transactions.

Monitoring systems should include (at a minimum) risk based rules based on the volume and value of transactions, to enable the detection of breaches of the transaction limits and wallet sizes outlined in Schedule 2 of the E-Money Order. The monitoring systems should also enable the EMI to detect and analyze suspicious and/or unusual activities and where deemed necessary, file a suspicious transaction/activity report (STR/SAR) with the FIUTT, in a timely manner[9].

In this regard, the transaction limits and wallet sizes for an individual and micro-enterprises will assist in mitigating the ML/TF risks. However, having regard to the larger wallet sizes, the EMI is expected to implement adequate AML systems commensurate with the intended level of risk identified at the on-boarding stage of the EMI customer. Monitoring systems should consider data on loading methods, potential spending patterns to identify high risk spending and conducting periodic assurance testing of agents to ensure adherence to the EMI's AML measures. See Appendix II outlining the on-boarding and ongoing monitoring steps that an EMI should take.

[6] Refer to Regulation 7(1) of the FOR
[7] Refer to Section 17(1) of the FIUTT Act
[8] The frequency of reports will depend on the volume of transactions executed by the entity and may be daily, weekly or monthly as appropriate.
[9] Refer to Section 55A(3) of the POCA.

APPENDIX I
IDENTIFICATION & VERIFICATION REQUIREMENTS

	MICRO TRANSACTIONS **MAXIMUM WALLET SIZE/ MONTHLY TRANSACTION LIMIT** **$5,000 / $5,000**	**MID VALUE TRANSACTIONS** **MAXIMUM WALLET SIZE/ MONTHLY TRANSACTION LIMIT** **$20,000 / $20,000**	**HIGH VALUE TRANSACTIONS** **MAXIMUM WALLET SIZE / MONTHLY TRANSACTION LIMIT** **$40,000 / $40,000**
INDIVIDUAL	**Record** customer's: • Full legal name; • Complete residential address; • Date and Place of Birth • Nationality Screen names of all individuals against lists of designated persons and high risk entities/countries.	**Record** customer's: • Full legal name; • Complete residential address; • Date and Place of Birth • Nationality **Obtain** a copy of one (1) form of valid national identification document to verify physical likeness, legal name, signature, date and place of birth. Screen names of all individuals against lists of designated persons and high risk entities/countries.	**Verify and Record** customer's: • Full legal name; • Complete residential address; • Date and Place of Birth • Nationality **Obtain** a copy of one (1) form of valid national identification document to verify physical likeness, legal name, signature, date and place of birth. **Verify** residential address by obtaining proof of address e.g. utility bill; hire purchase agreement; credit union or bank statement. Screen names of all individuals against lists of designated persons and high risk entities/countries.
	Micro Enterprises **MAXIMUM WALLET SIZE / MONTHLY TRANSACTION LIMIT** **$100,000 / $40,000**	**SMEs** **MAXIMUM WALLET SIZE/ MONTHLY TRANSACTION LIMIT** **$200,000 / $80,000**	**LARGE ENTERPRISES** **MAXIMUM WALLET SIZE/ MONTHLY TRANSACTION LIMIT** **$200,000/ $150,000**
BUSINESSES AS LISTED IN SCHEDULE 2 OF THE E-MONEY ORDER	Record customer's: • Full legal name; • Business address • Nature of business • Source of funds Obtain Formation Documents where applicable: • business registration certificate; • partnership agreement;	Record customer's: • Full legal name; • Business address • Nature of business • Source of funds Obtain Formation Documents where applicable: • business registration certificate; • partnership agreement;	Record customer's: • Full legal name; • Business address • Nature of business • Source of funds Obtain Formation Documents where applicable: • business registration certificate;

	• Articles of Association; • Certification of incorporation / Continuance / Amendment; • Notice of Directors and Notice of Business Address. Obtain one (1) form of valid national identification document for each individual /owner/partner/director/beneficial owner to verify physical likeness, legal name, signature, date and place of birth. If business is beneficially owned by a third party, record identity information of beneficial owner(s). Record and verify identity and address information for individuals who are politically exposed persons[10]. Screen names of all individuals and name of business against lists of designated persons and high risk entities/countries. **For Wallet sizes greater than $50,000** Obtain Statutory Returns where applicable: • Recent Annual Return; • BIR Tax Assessment Certificate; • NIB Certificate /Exemption Verify residential address of each individual by obtaining proof of address of individuals e.g. utility bill in individual's name, hire purchase agreement, credit union or bank statement. Verify Source of Funds for wallet. Obtain copies of audited financial statements or management accounts for the	• Articles of Association; • Certification of incorporation / Continuance / Amendment; • Notice of Directors and Notice of Business Address. Obtain Statutory Returns where applicable: • Recent Annual Return; • BIR Tax Assessment Certificate; • NIB Certificate /Exemption Obtain one (1) form of valid national identification document for each individual / owner / partner / director / beneficial owner to verify physical likeness, legal name, signature, date and place of birth. If business is beneficially owned by a third party, record and verify identity information of beneficial owner(s). Record and verify identity and address information for individuals who are politically exposed persons, and verify their source of wealth. Verify residential address of each individual by obtaining proof of address e.g. utility bill in individual's name; hire purchase agreement; credit union or bank statement. Verify source of funds for wallet. Obtain copies of audited financial statements or management accounts for the three (3) consecutive years immediately preceding the application.	• partnership agreement; • Articles of Association; • Certification of incorporation / Continuance / Amendment; • Notice of Directors and Notice of Business Address. Obtain Statutory Returns where applicable: • Recent Annual Return; • BIR Tax Assessment Certificate; • NIB Certificate /Exemption Obtain two (2) forms of valid national identification document for each Individual / owner/partner/director/beneficial owner to verify physical likeness, legal name, signature, date and place of birth. If business is beneficially owned by a third party/parties, record and verify identity information of beneficial owner(s). Record and verify identity and address information for individuals who are politically exposed persons, and verify their source of wealth. Verify residential address of each individual by obtaining proof of address e.g. utility bill in individual's name; hire purchase agreement; credit union or bank statement. Verify source of funds for wallet. Obtain copies of audited financial statements or management accounts for the three (3) consecutive years immediately preceding the application.

[10] Refer to definition of a Politically Exposed Person in Regulation 20 of the FORs.

	three (3) consecutive years immediately preceding the application. Conduct open source internet searches on all individuals and the business for negative news alerts.	Screen names of all individuals and name of business against lists of designated persons and high risk entities/countries. Conduct open source internet searches on all individuals and the business for negative news alerts.	Screen names of all individuals and name of business against lists of designated persons and high risk entities/countries. Conduct open source internet searches on all individuals and the business for negative news alerts.

APPENDIX II
PROCESS MAP OF EMI'S ON-BOARDING & MONITORING PROCESS