CENTRAL BANK OF TRINIDAD & TOBAGO

Guideline for Non-Bank Non-Financial Institutions

In Retail Payments

This Guideline is intended to provide standards of conduct for participants in the payment system and replaces the Payments System Guidelines 2 and 3 entitled the "Registration and Operation of Non-Interbank Payment Systems" and "Operation of Payment Service Providers", respectively.

Draft – April 29, 2020

TABLE OF CONTENTS

GLOSSARY

Acquirer	means the entity or entities that hold(s) deposit accounts for card acceptors (merchants) and to which the card acceptor transmits the data relating to the transaction. The acquirer is responsible for the collection of transaction information and settlement with the acceptors[1].
Agent	means a person acting in the name and on behalf of, and so representing one or more payment system operators or payment service providers.
Bill Payment Service Provider (BPSP)	means an entity that provides a bill payment acceptance or processing service for utility companies.
Business Continuity	refers to a payment system's arrangements which aim to ensure that it meets agreed service levels even if one or more components of the system fails or if it is affected by an abnormal external event.
Clearing	means the process of transmitting, reconciling and, in some cases, confirming transactions prior to settlement, potentially including the netting of transactions and the establishment of final positions for settlement.
Critical Service[2] Provider (CSP)	means a third-party service provider that is critical to the operations of a PSP or licensed financial institution. These institutions may fall under categories, such as information technology and messaging providers.
Custodian	means an entity, often a bank, that safe keeps and administers securities for its customers and that may provide various other services, including clearance and settlement, cash management, foreign exchange and securities lending.
Cyber Resilience	means the ability to anticipate, withstand, contain and rapidly recover from disruption caused by a cyber-attack.
Electronic Money (E-Money)[3]	means monetary value represented by a claim on the issuer, which is— (a) stored on an electronic device; (b) issued on receipt of funds of an amount

[1] Acceptors are any trading or service establishment that accepts, on its own behalf or on behalf of its network, the payment of goods or services via an electronic money instrument (BIS)
[2] Adapted from BIS – Assessment methodology for the oversight expectations applicable to critical service providers – Consultative Report https://www.bis.org/cpmi/publ/d115.pdf
[3] Section 2 of the FIA 2008

	not less in value than the monetary value issued; and (c) accepted as a means of payment by persons other than the issuer, so however that the funds referred to in (b) above shall not be treated as a deposit under this Act (FIA 2008);
Electronic Money Issuer (EMI)	means a category of persons (other than a licensee) who has been registered by the Central Bank to issue E-Money pursuant to the E-Money Ministerial Order.
Fintech	means technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services.
Interoperability	means the technical or legal compatibility that enables a system or mechanism to be used in conjunction with other systems or mechanisms. Interoperability allows participants in different systems to conduct, clear and settle payments or financial transactions across systems without participating in multiple systems.
Know-Your-Customer (KYC)	means the policies, procedures and systems instituted by financial institutions and regulated financial services providers in order to identify their customers.
Liquidity Risk	means the risk that a party will have insufficient funds to meet its obligations when they become due, although it may be able to do so at some time in the future.
Merchant Acquisition Service	means the facilitation of the acceptance and processing of payments for merchants.
Non-Bank Non-Financial Institution (NBNFI)	means an entity involved in the provision of retail payment services whose main business is not related to taking deposits from the public and using these deposits to make loans.
Non-Interbank Payment System Operator (NIPSO)	means an Operator of a payment system owned or operated by an entity, which is not a bank, which facilitates the electronic transfer of funds between or among entities other than banks.

Operational Risk	means the risk that deficiencies in information systems or internal processes, human errors, management failures or disruptions from external events will result in the reduction, deterioration or breakdown of services provided by a payment service provider.
Outsourcing	means the contracting or sub-contracting of one or more activities relating to the operation of a system or the issuance and management of a payment instrument to an independent third party. Such third party provides services to the issuer.
Oversight[4]	means in relation to a payment system, a public policy activity principally intended to ensure the safety, soundness, reliability and efficiency of the payment system in order to promote the effectiveness of monetary policy; contribute to the stability of the financial system by limiting the risk of systemic crises; and ensure the preservation of public confidence in money, money transfer mechanisms and the use of payment instruments.
Payment Card Industry Data Security Standard[5] (PCI DSS)	means measures that are designed to protect the entire acceptance and acquisition process. They provide broad coverage of data contained on cards, that is, both embossed data and data stored on stripes or chips. The aim is to combat all threats to security by taking account of the various ways in which different payment channels use card data.
Payment Initiation Service[6]	means an online service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.
Payment Instrument[7]	means every paper based, electronic or other means of effecting the transfer or withdrawal of money.
Payment Service	means a service which enables cash deposits and withdrawals, execution of a payment, the issue or acquisition of a payment instrument, the provision of a remittance service, and any other service functional to the transfer of money.

[4] Section 2 of the FIA
[5] https://www.bis.org/cpmi/publ/d102.pdf
[6] FCA Glossary of Terms
[7] FIA (2008)

Payment Service Provider (PSP)	means a person who provides a payment service and is registered or licensed to carry out one or more of the activities specified in Section 2.4.
Payment System[8]	means any organized set of infrastructure, persons, procedures and rules allowing the transfer of money, including by means of payment instruments, or the discharge of obligations on a gross or net basis.
Payment System User	means a person utilizing payment services in the capacity of either payer or payee, or both.
Payment Transaction[9]	means an act initiated by the payer or payee, or on behalf of the payer, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and payee.
Principles for Financial Market Infrastructure[10] (PFMI)	means the international standards for financial market infrastructures, i.e. payment systems, central securities depositories, securities settlement systems, central counterparties and trade repositories. Issued by the CPMI and the International Organization of Securities Commissions (IOSCO), the PFMI are part of a set of 12 key standards that the international community considers essential to strengthening and preserving financial stability.
Settlement	means the final, irrevocable transfer of funds between parties in a payments system. It is the stage where funds are moved from payer's account to payee's account. This involves: i) Collection and integrity checks of the claims to be settled; ii) Ensuring the availability of funds for settlement to occur; iii) Facilitating the settlement of the claims between payer and payee; and iv) iv. Logging and communication of settlement to the parties concerned.
Settlement Risk	means the risk that final settlement fails to take place, leading to a financial loss.
Significant Shareholder[11]	means a person who either alone or with one or more affiliates or relatives or connected parties is entitled, whether by agreement or otherwise, to exercise twenty percent or more of the voting power at any general

[8] Section 2 of the FIA
[9] FCA Glossary of Terms
[10] https://www.bis.org/cpmi/info_pfmi.htm
[11] Section 2 of the FIA

	meeting of the licensee and the terms "significant" and "significant interest" shall be construed accordingly.
Technology Service Provider (TSP)	means an entity or person who provides the hardware or software that allows PSPs to provide payment services/instruments as well as the clearing and settlement of instruments.
Wind Down	means the orderly discontinuation of one or more of an entity's services in a situation where it no longer continues providing its critical operations and services to participants.

1. INTRODUCTION

1.1 In 2012, the Central Bank of Trinidad and Tobago ("Central Bank"/ "Bank") issued four Payments System Guidelines[12], which provided standards of conduct for participants in the payment system. Due to the technological innovations taking place in the financial services industry in general and specifically in the payments space within recent times, the Central Bank has found it necessary to update its Guidelines governing Payment Systems[13]. Consequently, this Guideline for Non-Bank Non-Financial Institutions[14] in Retail Payments replaces the Payments System Guidelines 2 and 3 entitled the "Registration and Operation of Non-Interbank Payment Systems" and "Operation of Payment Service Providers", respectively.

1.2 The authority for the Central Bank to regulate payments systems, including remittance business, is derived from section 36(cc) of the Central Bank Act, Chap. 79:02 ("CBA"). In addition, the Central Bank has authority for oversight of the Interbank Payment Systems licensed under the Financial Institutions Act, 2008 ("the FIA").

1.3 Interbank Payment Systems[15], as well as payment services conducted by financial institutions licensed under the FIA ("licensees") are already subject to a licensing and regulatory framework. This Guideline seeks to provide guidance for Non-Bank Non-Financial Institutions that wish to provide payment services or operate a payment system[16].

[12] Guideline #1 – Licensing and Operation of Interbank Payment Systems – Nov 2012;
Guideline #2 – Registration and Operation of Non-Interbank Payment Systems – Nov 2012;
Guideline #3 – Operation of Payment Service Providers – Nov 2012; and
Guideline #4 – Oversight of Systemically Important Payment Systems – Dec 2012.

[13] This Guideline may be further amended following the approval of the E-Money Order that will allow certain categories of persons, other than licensed financial institutions (licensees), to issue e-money as accommodated by section 17(4) of the FIA which provides that:
"The Minister may, by Order, on the advice of the Central Bank, prescribe -
(a) the category of persons other than licensees, which may issue electronic money, subject to the approval of the Central Bank; and
(b) the requirements and criteria applicable to such persons."

[14] In this Guideline, unless otherwise specified a 'non-bank' refers to an entity not licensed under the Financial Institutions Act, 2008.

[15] An "Interbank Payment System" means any payment system between or among financial institutions, which facilitate the transfer of money or the discharge of obligations on a gross or net settlement basis.

[16] See a definition of a 'payment system' in section 3 of this Guideline.

1.4 For the purpose of this guideline, a person or entity providing a payment service, including those identified in Section 2.3 will be termed either a **Payment Service Provider ("PSP") or Non-Interbank Payment System Operator ("NIPSO")**.

2. PURPOSE AND SCOPE

2.1 The purpose of this Guideline is to detail Central Bank's expectations for the conduct of payment services in Trinidad and Tobago by Non-Bank Non-Financial Institutions.

2.2 As the Central Bank is responsible for supervising payment systems, Non-Bank Non-Financial Intuitions wishing to provide payment services are required to register with the Central Bank and adhere to the Terms and Conditions set out in this Guideline.

2.3 Accordingly, this Guideline applies to any entity that provides services along the payments chain including those providing software and hardware to facilitate payment services, specifically a Payment Service Provider ("PSP") and a Non-Interbank Payment System Operator ("NIPSO").

2.4 A PSP conducts generally one or more of the following activities:-

2.4.1 Issuing payment instruments e.g. debit or credit cards;

2.4.2 Account Opening services which include placing money on and withdrawing money from an account;

2.4.3 Merchant acquisition services which facilitate the acceptance and processing of payments for merchants;

2.4.4 Payment initiation services which allows the customer's/payer's account to be debited;

2.4.5 Execution of payment transactions;

2.4.6 Domestic money remittance[17]; (*see footnote*)

2.4.7 Cross border transfers[18]; (*see footnote*) and

2.4.8 Other services relevant to the provision of payment services not listed above including those providing hardware and software to facilitate payment services.

2.5 A NIPSO specializes in back-end clearing and settlement services, cooperating with banks and other payment service providers to whom they offer their services, usually in relation to different payment instruments. The principal activities of a NIPSO pertain to facilitating clearing and settlement.

3. APPLICATION FOR REGISTRATION

3.1 An application for registration as a PSP or NIPSO shall be in the specified format, accompanied by the application fee and shall include the requested documentation (see Schedule 1 and Appendix 1 and 2).

3.2 The Central Bank will generally seek to provide a response to an applicant within three (3) months of the receipt of all requested information and has the right to accept or reject any application for registration to operate as a PSP or NIPSO. Where the Central Bank rejects an application for registration to operate as a PSP or a NIPSO, the Central Bank shall provide clear reasons for its refusal to the applicant.

3.3 Where the Central Bank determines that the applicant has satisfied the criteria for registration pursuant to this Guideline, the applicant shall be registered and issued a Certificate of Registration ("Certificate") which may contain terms and conditions to be satisfied in a specified timeframe.

[17] Entities engaging in this activity will be required to also register with the Financial Intelligence Unit of Trinidad and Tobago;

[18] Subject to satisfying criteria to obtain a license from the Central Bank under the Exchange Control Act Chap.79:80 to conduct incidental foreign exchange conversions to facilitate international money remittance transfers and also be registered with the Financial Intelligence Unit of Trinidad and Tobago.

3.4 Where the Central Bank determines that the Registrant has not made sufficient progress to satisfy the terms and conditions of its registration, it may revoke the Certificate. Where the Registrant has made substantial progress, but was unable to satisfy all terms and conditions in the specified timeframe due to circumstances beyond its control, the Central Bank may extend the period for satisfaction of the conditions.

3.5 The Central Bank shall maintain a register of all registered PSPs and NIPSOs in any form it so chooses and shall publish on its website a list of registered entities.

3.6 Registrants will be required to pay an Annual Registration Renewal fee detailed in Schedule 1.

3.7 *Cancellation of Registration*

3.7.1 The Central Bank may remove an entity from the register where the PSP or NIPSO:

i. Has not commenced operations within six (6) months of the effective date of registration;

ii. Requests the cancellation of the registration;

iii. Ceases to engage in any business activity for six (6) months or more;

iv. Has furnished false statements or any other irregular information in the application for registration;

v. Has provided payment services other than in accordance with what was identified in the registration of the service;

vi. Provides payment services which are otherwise unlawful; or

vii. Any other reason(s) that the Central Bank may deem to be damaging to financial stability and public confidence in the domestic payments system.

3.8 Where the Central Bank intends to cancel a PSP's or NIPSO's registration on grounds as obtains in 3.7, the Central Bank will:

3.8.1 Give at least twenty-one (21) business days' notice in writing to the Registrant of its intentions, providing the reasons for so doing;

3.8.2 Consider any representations made in writing by the Registrant within that period; and

3.8.3 Communicate its final decision in writing within seven (7) business days of receipt of that representation.

3.9 Where a PSP's or NIPSO's registration has been cancelled, the PSP or NIPSO shall be removed from the register. The removal of a Registrant from the register shall be published on the Bank's website and may be published in at least one daily newspaper.

3.10 *The Application Process*

3.10.1 It is the applicant's responsibility to determine whether it is conducting an activity that would require it to registered with the Central Bank. However, if in doubt, the proposed applicant should contact the Payments Systems Oversight Division of the Central Bank at PSregistration@central-bank.org.tt for clarification.

3.10.2 Any entity seeking to be registered as a PSP or NIPSO must be a body corporate with a registered office in Trinidad and Tobago and must submit:

i. An application letter and application fee of $5,000.00.

ii. A completed application form (Appendix 2) together with the following documentation:

a. The business model detailing the type of payment services/instruments that will be provided inclusive of operating rules and regulations;

b. An organization structure and group chart showing the location of the applicant in the group (as applicable);

c. Audited financial statements for the most recent three (3) year period;

d. A detailed business plan including projected financial statements for the first three (3) years of operations, which should show that the applicant has the necessary systems, resources and procedures to operate as a PSP;

e. A certified copy of the Articles of Incorporation/Continuance, By-laws or other constituent documents of the applicant. This must also include its registered office address in Trinidad and Tobago;

f. Risk management policies for IT Security/Cybersecurity, business continuity, Anti Money Laundering/Combatting Terrorist Financing and internal controls;

g. Consumer Protection and redress policies and procedures, including a Disclosure policy;

h. A description of the governance arrangements (organizational chart) showing the position of and identifying executive and /or senior management officers;

i. A listing of shareholders who own 5% or more of the applicant (nominally or beneficially);

j. Personal Questionnaire and Declaration (PQD) forms for each director, officer of the applicant and individual significant shareholder owning 20% or more of the applicant (either nominally or beneficially);

k. Corporate Questionnaire and Declaration forms (CQDs) for each corporate shareholder owning 20% or more of the applicant (either nominally or beneficially);

l. A description of the operating structure including where applicable the planned use of agents and branches, outsourcing arrangements

and a description of the type and form of the entity's participation in the domestic payments system; and

m. Such additional information as the Central Bank may require.

3.10.3 Additional requirements for persons wishing to register as a NIPSO are available in Section 20 of this Guideline.

3.10.4 Upon receipt of an application, the Central Bank will review the form and attachments for completeness and advise of any outstanding documentation not submitted with the application within one (1) week. During processing of the application, the Central Bank may request additional information and/or meetings with the applicant to clarify information provided by the applicant.

3.10.5 The Central Bank will seek to complete its review on applications within three (3) months of the date of submission and subject to the receipt of all material information needed for the Central Bank to arrive at a decision.

3.10.6 Where an applicant does not respond to the Central Bank's request for information in a reasonable timeframe (such as six (6) months from the date of the initial application), the application shall be closed and a new application will be required to be submitted.

4. REGISTRATION REQUIREMENTS

4.1 PSPs and NIPSOs are required to satisfy the requirements in sections 4 through 16 of this Guideline at the application stage and on an ongoing basis.

4.2 Registrants are required to comply with all relevant laws, regulations and guidelines including those for Anti-Money Laundering / Countering Terrorist Financing and Proliferation Financing (AML/CFT/CPF)[19] and the Central Bank's Fit and Proper

[19] https://www.central-bank.org.tt/core-functions/financial-stability/amlcft

Guideline, 2019.

4.3 Registrants are expected to also advise users/participants and their representatives about adherence to relevant laws and guidelines, including those pertaining to anti-money laundering and terrorist financing.

4.4 All registered PSPs and NIPSOs shall be required to submit data on their operations to the Central Bank in such form, manner and frequency as the Central Bank may require.

4.5 *Restrictions*

4.5.1 A person registered as a PSP or a NIPSO is prohibited from:

i. Co-mingling funds with any other entity or person;
ii. Buying, selling or dealing in foreign currency;
iii. Granting of credit;
iv. Issuing/allowing joint accounts;
v. Paying interest on accounts; and
vi. Issuing instruments in currencies other than the Trinidad and Tobago Dollar (TTD).

5. GOVERNANCE REQUIREMENTS

5.1 All entities must be a body corporate with its registered office in Trinidad and Tobago.

5.2 Entities desirous of operating as a PSP or a NIPSO shall establish adequate governance arrangements, which are effective and transparent, to ensure the continued integrity of their payment services. All directors, officers, significant and

controlling shareholders of the applicant, must be fit and proper[20] and subject to the Central Bank's approval process.

5.3 The business shall be directed by a minimum of two persons, at least one of whom must possess the requisite experience and technical knowledge to direct the business activities.

5.4 Registrants should refer to the Central Bank of Trinidad and Tobago's Corporate Governance Guidelines[21] and Principle #2 of the Principles for Financial Market Infrastructure (PFMI)[22] for Governance requirements.

6. RISK MANAGEMENT

6.1 Registrants shall develop and implement a Board approved risk management framework that includes procedures to enable:

6.1.1 adequate identification, measurement, monitoring and management of the range of risks that may arise in its operations, as well as the timeframe for periodic reviews. This includes but is not limited to credit, liquidity, general business, operational, settlement and cyber risk;

6.1.2 identification of scenarios that may potentially disrupt operations and the provision of services and conduct suitable stress testing of these scenarios;

6.1.3 strategies for recovery and/or wind down as appropriate. Measures to ensure operational reliability shall include:

i. an appropriate system(s) which is robust in its design, development, testing, implementation and monitoring;

[20] See the Fit and Proper Guideline issued by the Central Bank https://www.central-bank.org.tt/sites/default/files/circular_letters/Fit_and_Proper_.pdf
[21] https://www.central-bank.org.tt/sites/default/files/page-file-uploads/Corporate%20Governance_0.pdf
[22] PFMIs are the international standards for assessing payments systems operating Financial Market Infrastructures. https://www.bis.org/cpmi/publ/d101a.pdf

ii. strong internal controls for systems and personnel administration and a risk management framework that addresses operational, settlement, liquidity, IT/ cyber and AML/CFT/CPF (collectively 'AML' hereafter) risks;

iii. comprehensive and well documented operational and technical procedures to ensure operational reliability;

iv. clearing and settlement arrangements as appropriate;

v. robust business continuity, including a reliable back-up system;

vi. robust systems to ensure cyber resilience; and

vii. adequate accounting systems and proper reconciliation processes.

7. SETTLEMENT AND LIQUIDITY ARRANGEMENTS

7.1 Registrants must provide clear and certain final settlement. Additionally, all Registrants must have sufficient liquidity to meet customer demands, mitigate loss of customers' funds due to fraud or error and to ensure that transactions can be settled safely and efficiently.

7.2 *Settlement Arrangements*

7.2.1 Registrants must provide detailed information on their settlement arrangements. As such, Registrants must:

i. identify their Settlement agent;

ii. identify their Settlement times;

iii. ensure the maintenance of accurate settlement and transaction records, which must be held for no less than six (6) years and should be made available to the Central Bank upon request.

7.2.2 Where the applicant is responsible for settlement, the Operating Rules and Regulations (ORR) of the entity should clearly define the point at which

transactions are settled and irrevocable; the process for managing unsettled payments and returns as well as changes to prescribed operating procedures if they occur.

7.2.3 Final settlement should occur by no later than the end of the value date and participants of the system should be advised of final settlement of their transactions as far as possible.

7.3 Liquidity Arrangements

7.3.1 Registrants must provide evidence of adequate liquidity and implement liquidity risk management measures, such as:

i. having a segregated custodian account at a licensed commercial bank specific for settlement purposes only[23];

ii. holding liquid net assets funded by equity equal to at least six (6) months of current operating expenses as per PFMI standards.

iii. implementing a robust framework to manage liquidity risks from its participants, settlement agents and other entities; and

iv. where possible, making use of analytical tools to identify, measure and monitor settlement and funding flows on a timely basis.

7.4 Safeguarding of Customers' Funds

7.4.1 The funds identified in 7.3.1 should be ring fenced, unencumbered and readily and easily available. The Central Bank may impose further requirements for the safeguarding of funds relevant to losses.

[23]The Central Bank may require an e-money issuer to keep its liquid assets in a custodian account at more than one financial institution in the interest of protecting customers.

8. ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM AND PROLIFERATION FINANCING (AML/CFT/CPF)

8.1 Registrants must adhere to Legislation and Guidelines on AML. including and not limited to:

8.1.1 The Central Bank's Guidelines on AML/CFT[24];

8.1.2 AML/CFT/CPF legislation, regulations and Guidelines[25].

8.2 All Registrants must submit their Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) policy detailing their Know Your Customer (KYC) and Customer Due Diligence (CDD) procedures to the Central Bank.

8.3 PSPs and NIPSOs shall ensure that any third party/agent acting on their behalf comply with relevant requirements and legislation of Trinidad and Tobago.

9. USE OF AGENTS / AGENT MANAGEMENT

9.1 All Registrants shall ensure compliance with all relevant agreements and remain fully liable for any act of their agents and any third parties to which they have outsourced activities.

9.2 Agents acting on behalf of Registrants must inform customers of their authorisation to act as agents of the Provider.

9.3 Registrants must submit copies of any agent agreements to the Central Bank.

Further details on the Use of Agents and Agent Management are available in Schedule 2 – "Agent Arrangements and Management."

[24] https://www.central-bank.org.tt/sites/default/files/page-file-uploads/Draft%20AML%20CFT%20Guideline%20_July%202017_1.pdf
[25] https://www.central-bank.org.tt/core-functions/financial-stability/amlcft

10. INFORMATION AND COMMUNICATIONS TECHNOLOGY STANDARDS AND SECURITY (ICT)

10.1 All Registrants shall adhere to:

10.1.1 The Central Bank's Guideline on Security Systems for Safeguarding Customer Information;[26]

10.1.2 International Organization for Standardization and International Electro Technical Commission Standard 27002 (ISO/IEC 27002); and

10.1.3 The PCI Data and Security Standards (PCI DSS) once engaging in, any card activities.

10.2 Registrants must:

10.2.1 Complete and submit the Central Bank's ICT Standards and Security Questionnaires placed on the Central Bank's website; and

10.2.2 Develop, document in writing and implement an information security programme that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities.

10.3. *Cyber Risk and Cyber Security*

10.3.1 Registrants must implement a clear and comprehensive cyber resilience framework. This framework should place a high priority on safety and efficiency of operations, cyber resilience objectives, as well as, the requirements for people, processes and technology necessary to manage cyber risks. This framework should include procedures for:

i. timely communication and collaboration with relevant stakeholders.

[26] https://www.central-bank.org.tt/sites/default/files/page-file-uploads/Security%20Systems%20for%20Safeguarding%20Customer%20Information.pdf

This should be supported by clearly defined roles and responsibilities of the PSP's/NIPSO's board (or equivalent) and its management.

ii. identification and classification of business processes, information assets, system access and external dependencies towards better understanding of the PSP's/NIPSO's internal situation. This will include the cyber risks that the entity bears from and poses to all stakeholders with whom its system may be interconnected.

iii. implementation of appropriate and effective controls and design systems and processes consistent with cyber resilience and information security practices.

iv. implementation of monitoring and processing tools for the detection of cyber incidents.

v. rigorous testing of all elements of the cyber resilience framework to ensure efficiency and effectiveness.

vi. monitoring of the cyber threat landscape, and acquiring actionable threat intelligence to validate its risk assessments, strategic direction, resource allocation, processes, procedures and controls with respect to building cyber resilience.

vii. ongoing re-evaluation and improvement of the PSP's or NIPSO's cyber resilience framework.

11. OPERATIONAL REQUIREMENTS

11.1 Registrants should mitigate the impact of both internal and external operational risks, with appropriate systems, policies, procedures, and controls.

11.2 Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. As such, Registrants should:

11.1.1 establish a robust operational risk-management framework with appropriate systems, policies, procedures, and controls to identify, monitor, and manage operational risks;

11.1.2 have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives;

11.1.3 ensure that it has scalable capacity adequate to handle increasing stress volumes and to achieve its service-level objectives;

11.1.4 ensure interoperability arrangements are in place that allows participants in different systems to conduct, clear and settle payments or financial transactions across systems; and

11.1.5 have separate records and accounts for each activity in the case of multiple payment services.

11.3 Registrants must have a Business Continuity Plan (BCP) that addresses: Events posing a significant risk of disrupting operations, including events that could cause wide-scale or major disruption; The use of a secondary site which should be designed to ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events (as per PFMI standards). The PSP should regularly test these arrangements; and Change-management and project-management processes to mitigate operational risk arising from modifications to operations, policies, procedures, and controls.

12. OUTSOURCING AND THIRD PARTY ARRANGEMENTS

12.1 Outsourcing of a service or business operation does not exempt the Registrant from the responsibility of ensuring that their data/business operations is properly secured. Therefore, Registrants are required to inform the Central Bank of all outsourcing operations and activities.

12.2 The Registrant should have clearly defined policies, procedures or service level agreements where applicable with the Cloud Service Providers for all security

requirements, operations, management of data storage, and reporting.

12.3 As such, Registrants must comply with the following upon registration:

12.3.1 Complete and submit the ICT Outsourcing Questionnaire found on the Central Bank's website.

12.3.2 Provide the Central Bank with any agreements such as, but not limited to, Service Level Agreements (SLAs).

12.3.3 Where Cloud Service Providers are utilized the PSP and NIPSO should ensure that they adhere to the PCI Data Security Standards (PCI DSS), Cloud Computing Guidelines as well as, the Central Bank's Guideline on Security Systems for Safeguarding Customer Information.

13. REGULATORY OVERSIGHT AND REPORTING REQUIREMENTS

13.1 Registrants must provide the Central Bank with access to premises, records, systems, processes and people for reviewing the conduct of all permissible activities at all reasonable times.

13.2 Registrants must submit requested reports to the Central Bank by the stipulated deadlines. These will include: -

13.2.1 *Annual Reports*

i. Audited Financial Statements by a duly certified auditor within three (3) months of its financial year-end; and

ii. External Auditors' Report including a report on AML/CFT compliance within four (4) months of its financial year-end.

13.2.2 *Monthly Reports*

i. PSPs would be required to complete the CB74 Statistical Return. The

return captures data on the volume and value of payments processed.

ii. NIPSOs would be required to complete the CB71 Statistical Return. The Return captures data on volumes and values of operator transactions including direct debits and credits, returns, rejects and fee structure.

13.3 Monthly Reports are due by the **15th working day** following the end of the reporting period in both printed and electronic format. The printed return (i.e. hard copy) must be signed by an officer, stamped and forwarded to:

The Manager
Statistics Department
Central Bank of Trinidad & Tobago
Eric Williams Plaza
Independence Square
Port of Spain

The electronic copy (i.e. a soft copy) is to be encrypted and emailed to payments2@central-bank.org.tt.

13.4 A Registrant must notify the Central Bank within 1 day of the occurrence of any of the following events:

13.4.1 Any legal proceeding instituted against the Registrant;

13.4.2 Any disciplinary action taken against an agent/participant;

13.4.3 Any failure of the operation of the service including disruptions in the availability of the service to end-users; and failure of settlement; and

13.4.4 Any cyber incidents or threats.

13.5 The Registrant should within 5 days of the occurrence of the event, submit a report to the Central Bank detailing the circumstances surrounding the event, the corrective actions taken, and any follow-up actions taken or intended.

14. MARKET CONDUCT REQUIREMENTS

14.1 *Consumer Protection*

14.1.1 All Registrants must establish a customer redress and resolution system that is adequate to resolve complaints and issues in a timely manner.

14.1.2 Provide a means of treating with payment service users' complaints; resolving disputes no later than 30 days, from the date the complaint was made) in accordance with the laws of Trinidad and Tobago and standard setting bodies such as:

i. The National Consumer Policy[27];

ii. The proposed Consumer Protection and Empowerment Act; and

iii. The Bureau of Standards Quality Management - Customer Satisfaction Guidelines (TTS/ISO 10003:2008 and TTS/ISO10001:2008).

14.1.3 A Registrant must notify users of changes to payment services at least one (1) month prior to the effective date. Temporary changes to payment services offered must be communicated to users as soon as is practicable.

14.1.4 Ensure that the personalized security features of the payment instrument are not accessible to persons other than the user to whom the instrument has been issued.

14.1.5 Each Registrant must facilitate clear identification of transactions to users in a manner that is understandable and accessible to the user. Such identification must include:

i. References which will enable the user to identify the payment transaction including the date and time of transaction;

[27] https://tradeind.gov.tt/national-consumer-policy-tt/

ii. The amount of each transaction; and

iii. Charges payable in respect of the transaction.

14.2 Disclosure Requirements

14.2.1 At a minimum, the following information should be provided to users of the registrant's service:-

i. Conditions for the use of the service such as Terms of Use, User Service Agreements and Privacy Policies;

ii. Charges and/or fees associated with the service;

iii. Information necessary for customers to contact the issuer or its agent in the event of a query or concern.

iv. All necessary and appropriate documentation to facilitate participants' understanding of the system's rules and procedures and the risks users face from participating in the system;

v. The responsibilities and liabilities of the user and Registrant; and

vi. The timeframe within which the service may be reasonably executed.

14.2.2 The responsibilities of the parties concerned in the offering and use of payment services must be clearly documented, and agreed upon prior, to its use. The PSP/ NIPSO at a minimum should: -

i. Provide a means of contact to enable the user to notify the institution in the event of theft, loss or unauthorised usage of the service or any associated instrument or equipment used to access the service; and prevent any further use of the instrument or service upon receipt of such notification;

ii. Ensure that the user is aware of the liability of the Registrant for the value of transactions where:

a. The Registrant has failed to make the appropriate information

available to the user concerning the payment transaction;

b. A payment transaction was unauthorized subject to a. above; and

c. The Registrant failed to provide the user with a means of notification to be used in the event of the theft, loss or unauthorised usage of the service or any associated instrument or equipment used to access the service.

15. ADDITIONAL CRITERIA FOR NIPSOs

15.1 *Operating Rules and Regulations (ORR)*

15.1.1 Where the operator is responsible for settlement, the Operating Rules and Regulations (ORR) must address:

i. Objectives of safety and efficiency;

ii. Default Mechanisms for participant default regarding settlement of payments;

iii. Collateral to mitigate against participant's credit and liquidity risks; and

iv. Wind down Procedures in the event of closure of the business or a participant's exit from the system.

15.2 *Collateral*

15.2.1 The operator should hold collateral to cover participant default of at least the highest daily settlement value as calculated every six (6) months. The funds must be kept in cash and deposited into an account that facilitates immediate *withdrawals.*

15.3 *Prudent Management of Funds*

15.3.1 All NIPSOs should observe the following minimum standards to ensure

prudent management of funds:

i. Ensure that they have sufficient liquidity for their daily operations.

ii. Ensure that funds collected from or on behalf of participants are managed separately from the operators working capital funds. At no point in the clearing or settlement process should the NIPSO have access to or hold the consumer's or participant's funds;

iii. All charges or credits should be debited or credited immediately to the customer account at the time of transaction or redemption.

iv. Transactions processed by NIPSOs should be settled amongst the participants safely and efficiently.

16. OVERSIGHT ASSESSMENT

16.1 Section 36 (cc) of the CBA gives the Central Bank the authority to supervise the operations of Payments Systems. As such, the Central Bank will assess all Registrants against the CPMI-IOSCO PFMI requirements, which provide for the safe and sound operation of payment systems. These details are specified in the Framework for Oversight of the Payments Systems in Trinidad and Tobago[28].

17. EFFECTIVE DATE

17.1 The Guideline becomes effective from the date of issue.

17.2 The Central Bank will review the Guideline from time to time to ensure the it continues to reflect international best practices aimed at maintaining the stability of the financial system and efficiency of the payments system.

[28] The Framework for Oversight of the Payments Systems in Trinidad and Tobago is being finalized and will replace the previous Guideline No. 4.

SCHEDULES

Schedule 1

Application & Registration Fees

The fees applicable to Registrants and their Agents are as follows:

	Application Fee	Initial Registration Fee	Annual Registration Fee
Payment Service Provider (PSP)	TTD5,000		TTD15,000
Non Interbank Payment System Operator (NIPSO)	TTD5,000	TTD50,000	TTD25,000

Schedule 2

Agent Arrangements and Management

Agent Arrangements

Registrants that intend to utilize Agents shall submit the following information to the Central Bank:

1.
2. List of Agents used;
3. The results of the due diligence conducted by the registrant to select the said agent(s);
4. The proposed geographic location of the agent/agent network;
5. The services to be provided by the agent;
6. Copies of:
    a. certificate of incorporation/registration of business;
    b. evidence of a registered office in Trinidad and Tobago; and
    c. memorandum/articles of association.
7. Documents demonstrating the Agent's financial soundness. These should include one of the following where applicable:
    a. audited financial statements;
    b. management accounts; or
    c. cash flow statements.
8. Copy of the Agency agreement, between the Agent and the registrant, containing at minimum:
    a. a clear indication of the duties and responsibilities of each party;
    b. any compensation arrangements;

c. the scope of work to be performed by the Agent;

d. a statement that the registrant is responsible and liable for the actions and/or omissions of an Agent providing the services on its behalf;

e. a statement that the Agent shall ensure safe-keeping of all relevant records and ensure that the records are, at pre-specified regular intervals, moved to the registrant who shall ensure safekeeping of these records for at least six (6) years; and

f. an agreement by both parties to provide unrestricted access to the Central Bank to review the Agent's internal systems, information, data and documents relevant to the conduct of permissible activities.

9. The policies and procedures approved by the registrant for the provision of services through the Agent including anti-money laundering and combatting terrorist financing controls to be implemented by the Agent;
10. A description of the technology to be used for delivering Agency services;
11. A risk assessment report of the provision of permissible activities through the Agent including the control measures that will be applied to mitigate the risks;
12. A report regarding internal controls to be used for the agency business which must be reviewed by an auditor on an annual basis; and
13. Any further information that the Central Bank may consider necessary.

Agent Management

The registrant must:

1. Maintain systems, policies and procedures, including risk management policies relevant to ML/TF/PF risk, to exercise effective internal control over the provision of services by its Agents;
2. Ensure that there is adequate training and support for its Agents with a view to providing safe and efficient services to customers;

3. Accept liability for the conduct of their Agents performed within the scope of the relevant agency agreement and the agreement shall not exclude this liability;
4. Submit an annual report prepared by an external auditor, in respect of the operations of its Agents, to the Central Bank within four (4) months from the end of each financial year;
5. Demonstrate its ability to track and maintain records of the payments transactions carried out by each Agent it uses to the satisfaction of the Central Bank; and
6. Maintain a list of Agents used, and information relevant to these agents including name, address, GPS coordinates, telephone contact (including the contacts and addresses for each outlet of the agent at which it will provide services on behalf of registrant) which shall be submitted to the Central Bank on a quarterly basis.

APPENDICES

Appendix 1

1. SAMPLE APPLICATION LETTER - PSP

DATE

From: (Applicant's Name and Registered address)

To: Inspector of Financial Institutions,
Financial Institutions Supervision Department
Central Bank of Trinidad and Tobago
Eric Williams Plaza, Independence Square,
PO Box 1250,
Port of Spain.

Dear Sir,

Application to register as a Payment Service Provider

We hereby submit an application to register as a Payment Service Provider (PSP) in accordance with this Payment System Guideline issued under Section 36 (cc) of the Central Bank Act Chapter 79:02.

We declare to the best of our knowledge that the information furnished is true, correct and complete.

Name:

Designation:

Company Stamp:

2. SAMPLE APPLICATION LETTER - NIPSO

DATE

From: (Applicant's Name and Registered address)

To: Inspector of Financial Institutions,
Financial Institutions Supervision Department
Central Bank of Trinidad and Tobago
Eric Williams Plaza, Independence Square,
PO Box 1250,
Port of Spain.

Dear Sir,

Application to register as a Non-Interbank Payment System Operator

We hereby submit an application to register as a Non-Interbank Payment System Operator (NIPSO) in accordance with this Payment System Guideline issued under Section 36 (cc) of the Central Bank Act Chapter 79:02.

We declare to the best of our knowledge that the information furnished is true, correct and complete.

Name:

Designation:

Company Stamp:

Appendix 2

APPLICATION FORM AND CHECK LIST

	Date of Submission: Name of Contact Person: Position of Contact person: *Complete and confirm that the following documents are enclosed:*	Enclosed (√)
1	GENERAL DETAILS	
1.1	Registered Company Name:	
1.2	Trade name (if different from above):	
1.3	Registered Business Address:	
1.4	Telephone Number:	
1.5	Email Address:	
1.6	Institution Website:	

	Date of Submission: Name of Contact Person: Position of Contact person: *Complete and confirm that the following documents are enclosed:*	Enclosed (√)
1.7	Notification of the statute under which the entity is incorporated/established. For example, Companies Act etc.	
2	LEGAL AND COPORATE GOVERNANCE ARRANGEMENTS	
2.1	A certified copy of the Certificate of Incorporation, Articles of Incorporation/Continuance, By-laws, Notice of Directors or any other constituent document, including any amendments.	
2.2	Notice of the principal place of business (including telephone and fax numbers, email address and website).	
2.3	A listing of the current Board of Directors and Senior Management of the Company and Corporate Controllers of the company as well as completed Personal Questionnaire and Declaration (PQD) forms for each named individual person. The list should clearly identify independent directors of the Company and Controllers of the Company.	
2.4	A listing of shareholders who own 20% or more of the paid-up capital inclusive of the respective size of their holdings.	
2.5	The name, address, nationality, experience, police certificate and other relevant information pertaining to each director and senior management officer and corporate controller of the entity.	

	Date of Submission: Name of Contact Person: Position of Contact person: *Complete and confirm that the following documents are enclosed:*	Enclosed (√)
2.6	A copy of the company's most recently filed Annual Return with the Registrar of Companies (if applicable).	
3	GROUP AND ORGANIZATIONAL STRUCTRE	
3.1	Organizational Chart of the Board of Directors, Senior Management and Corporate Controllers of the Company.	
3.2	The Governance and Group structure for the entity, including a listing of all affiliated companies and the nature of the relationship.	
3.2	Corporate Questionnaire and Declaration Forms (CQDs) for each corporate shareholder owning 20% or more of the applicant (either nominally or beneficially).	
4	BUSINESS OPERATIONS	
4.1	A detailed schematic diagram showing the process flow of transactions and information on the entity's platform/s for each of the products and/or services to be offered including details on various uses of the proposed products and/or services.	

	Date of Submission: Name of Contact Person: Position of Contact person: *Complete and confirm that the following documents are enclosed:*	Enclosed (√)
4.2	The business model, as well as, the Operating Rules and Regulations governing the entity's operations.	
4.3	A detailed Business Plan including projected financial statements for the first three (3) years of operations, Balance Sheet, Income and Cash Flow Statements.	
4.4	Audited Financial Statements – three 3 years (for existing entities).	
4.5	Copies of any agreements entered into with partners, providers, or customers where applicable.	
4.6	Evidence that the registrant has the required initial capital of TT$ XXXXXX.	
5	RISK MANAGEMENT	
5.1	Risk Management Policy and Framework.	
5.2	Policies addressing: Cyber resilience, business continuity, and internal controls with emphasis on the safety and efficiency of operations. Cyber resilience objectives and the requirements for the people, processes, and technology necessary to manage cyber risk.	

	Date of Submission: Name of Contact Person: Position of Contact person: *Complete and confirm that the following documents are enclosed:*	Enclosed (√)
5.3	Anti-Money Laundering and Combatting Terrorist Financing (AML/CTF) policies.	
5.4	Details on Consumer Protection and Disclosure information where required. This will include at a minimum Terms of Use, User Service Agreements and Privacy Rules, charges and/or fees associated with the service, and information that will facilitate participants' understanding of the service rules and procedures and the risks users/clients will face from their usage of each of the entity's products and services.	
6	INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)	
6.1	The Central Bank's *Information and Communications Technology Infrastructure and Security Standards* document.	
6.2	Technology arrangements inclusive of the entity's detailed network infrastructure diagram, information flows as it related to transactions and data, and authentication, validation and encryption mechanisms employed.	
7	OUTSOURCING ARRANGEMENTS	
7.1	Details on the arrangements with each outsourced entity where applicable.	

	Date of Submission: Name of Contact Person: Position of Contact person: *Complete and confirm that the following documents are enclosed:*	Enclosed (√)
7.2	The completed Central Bank's *Information and Communications Technology Outsourcing* Questionnaire.	
8	AGENT AND AGENT MANAGEMENT	
8.1	All items requested in Schedule 2 of this Guideline "Agent Arrangements and Management".	
8.2	A list of Agents used, and information relevant to these agents including name, address, GPS coordinates, telephone contact (including the contacts and addresses for each outlet of the agent at which it will provide services on behalf of registrant.	
9	SETTLEMENT AND LIQUIDITY REQUIREMENTS	
9.1	Information on the applicant's settlement agent.	
9.2	Information on the applicant's settlement times.	

	Date of Submission: Name of Contact Person: Position of Contact person: *Complete and confirm that the following documents are enclosed:*	Enclosed (√)
9.3	Evidence of adequate liquidity in a segregated bank account (specifically for settlement.	
9.4	Liquidity Risk framework.	
9.5	Evidence that steps to safeguard customers' funds have been implemented.	

REFERENCES

1. Central Bank of Bahamas, *General Information and Application Guidelines for Providers of Electronic Retail Payment Instruments and Electronic Money products (Payment Service Providers*, July 2017 http://www.centralbankbahamas.com/download/023811100.pdf
2. Bank of Jamaica, *Payment System Guidelines and Application for Authorization*, 2013 http://www.boj.org.jm/financial_sys/payments_systems_policy.php
3. Bank of Jamaica, *Guidelines for Electronic Retail Payment Services*, 2018 http://www.boj.org.jm/uploads/news/2019_erps_guidelines_for_electronic_retail_payment_services_(erps_2).pdf
4. Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions (BIS) *Glossary of Terms* - Payment and Settlement Systems https://www.bis.org/cpmi/glossary_030301.pdf
5. Committee on Payment and Settlement Systems, Technical Committee of the International Organization of Securities Commissions, *Principles for Financial Market Infrastructures*, April 2012 https://www.bis.org/cpmi/publ/d101a.pdf
6. Monetary Authority of Singapore (MAS) *Consultation Paper on Proposed Payment Services Bill* http://www.mas.gov.sg/~/media/resource/publications/consult_papers/2017/Annex%20B%20to%20Consultation%20on%20Proposed%20Payment%20Services%20Bill%20MAS%20P0212017.pdf
7. *National Consumer Policy of Trinidad and Tobago* https://tradeind.gov.tt/national-consumer-policy-tt/
8. Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions Consultative report, June 2016, *Guidance on cyber resilience for financial market infrastructures* https://www.bis.org/cpmi/publ/d146.pdf
9. *PCI DSS Cloud Computing Guidelines,* 2013 version 2.0 updated (2018)

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf

10. Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions, Principles for financial market infrastructures: *Assessment methodology for the oversight expectations applicable to critical service providers*, December 2014 https://www.bis.org/cpmi/publ/d123.pdf
11. https://www.merchact.com/payment-aggregator-vs-payment-gateway-whats-difference-2/
12. Electronic Payments Law, December 2011, https://www.electronicpaymentslaw.com/aggregator-rules-evolve/
13. Reserve Bank of India – *Press Release on Payment System Aggregators*, March 2017 https://www.rbi.org.in/scripts/FS_PressRelease.aspx?prid=40004&fn=9
14. Central Bank of Kenya – *E Money Regulations*, 2013 https://www.centralbank.go.ke/images/docs/NPS/Regulations%20and%20Guidelines/Regulations%20-%20E-%20Money%20regulations%202013.pdf
15. Bank of Ireland – *Guidance Note on Completing an Application*, April 2018 https://www.centralbank.ie/docs/default-source/Regulation/industry-market-sectors/Electronic-Money-Institutions/Authorisation-Process/psd2-guidance-note.pdf?sfvrsn=3
16. National Payment System Act, 2018, (Act No. 13 of 2018), Guyana
17. Payment and Settlement Systems Regulations, 2014, Bangladesh