Guidelines for Electronic Retail Payment Services (ERPS 2)

Issue Date: ***1 November 2018***
Effective Date: ***1 February 2019***

Foreword

The 2019 Guidelines for Electronic Retail Payment Services (ERPS 2) represent the first update of the Guidelines since initial publication by Bank of Jamaica (Bank) on 1 February 2013.

The Bank, in recognition of changes and developments in the financial services industry and particularly in the retail payment services sector, requested comments and suggestions for modification of the Guidelines from twenty-five (25) major stakeholders. Following consultations and follow up discussions, written comments and feedback were received from nine (9) stakeholders. The Bank, after taking into consideration the feedback from stakeholders, now publishes the revised 2019 Guidelines for Electronic Retail Payment Services (ERPS 2), implementation of which takes effect on 1 February 2019.

The purpose of ERPS 2, is to support the continued effort of the Bank to foster the design, development and implementation of electronic retail payment systems, which take advantage of available technology, to provide more efficient payment services in a safe, secure and competitive environment. The ultimate objective is to ensure that consumers are provided with a range of payment services and instruments to satisfy current and projected demands.

ERPS 2 provides the operating parameters that must be satisfied by providers who intend to offer electronic retail payment services in Jamaica. Applications must be made to, and authorisation secured from, the Bank before commencement of operations. Application forms and other information pertaining to the authorisation process are available on the Bank's website.

The Bank reserves the right to modify ERPS 2 where considered necessary, subject to the provision of appropriate notification to stakeholders.

Queries or requests for clarification should be sent by electronic mail to payment.system@boj.org.jm.

Livingstone Morrison, OD
Deputy Governor
Bank of Jamaica

Table of Contents

Contents

1. Introduction

1.1. The purpose of the 2019 Guidelines for Electronic Retail Payment Services (ERPS 2) is to provide a revised framework to support the introduction of new payment instruments and services, and the continued development of the payment services sector in Jamaica. Bank of Jamaica (Bank), in discharging its responsibility for payment system oversight, will apply ERPS 2 to promote consistency of treatment of all Payment Service Providers (PSPs) and the electronic retail payment instruments and services that they are authorised to offer to consumers.

1.2. Entities wishing to operate as PSPs must satisfy the requirements outlined in ERPS 2 to secure the necessary authorisation from the Bank. Importantly, ERPS 2 provides for authorisation of different categories of PSPs to include issuers of payment instruments and services, payment initiation service providers and merchant acquirers.

1.3. The Bank will continue to work with all stakeholders to ensure the continued relevance of ERPS 2 as an appropriate framework for facilitating the continued growth and development of the payment services industry.

2. Authority

2.1. ERPS 2 is issued in accordance with the provisions of the Payment Clearing and Settlement Act, 2010 (PCSA) under which the Bank holds responsibility for oversight of the National Payment System (NPS). Through the execution of its oversight function, the Bank seeks to promote the prudent and safe management of retail payment services as part of the process of ensuring the safety and soundness of the NPS and the proper functioning of the financial system in general.

2.2. Authorisation in accordance with ERPS 2 does not provide a basis for conducting deposit taking business, which may only be conducted by deposit taking institutions (DTIs) based on approval by the Bank.

3. Objectives

2.3. The objectives of ERPS 2 are to:

a. define authorisation requirements that will be applied by the Bank;

b. outline the standards to be observed by PSPs;

c. foster and maintain public trust and confidence in authorised retail payment systems;

d. promote financial inclusion; and

e. promote competition in the retail payment services sector.

4. Definitions

Definitions in alphabetical order are detailed in the following subsections.

4.1 *Agent* means a person who is authorised by the Bank under Section 11 of ERPS 2 to provide payment services on behalf of a PSP.

4.2 *Custodian Account* is a special purpose account or pooled account held for the PSP, where the customers of the PSP are the beneficiaries, and where funds of such customers are pooled for the purpose of settlement and management of the payment services that the PSP agree to provide to its customers. The amounts due to each customer, the aggregate of which constitute the total balance held in the custodian account, will be treated as sub-accounts for individual coverage by the Jamaica Deposit Insurance Corporation (JDIC).

4.3 *Customer* means a person to whom an electronic retail payment instrument has been issued by a PSP or any person who uses an electronic retail payment instrument or an electronic payment service.

4.4 *E-money* means electronically, including magnetically, stored monetary value on any device or instrument or server as represented by a claim on the PSP, which is issued on receipt of funds for the purpose of making payments and which is accepted as a means of payment by persons other than the PSP. This includes e-money stored on a device such as a SIM card or a server and accessible via telephone, internet or other access devices, cards, and other similar instruments but excludes any electronic means to permit transfers to/and from a deposit or current account held by a DTI.

4.5 *Electronic Retail Payment Instrument* means a tool or set of procedures for enabling the transfer of funds, with the exception of credit cards, from a payer to a payee where the payer and the payee may be one and the same person.

4.6 *Electronic Retail Payment Service* means the operation and management of activities relating to the use of an electronic retail payment instrument including the rules, standards and procedures governing the relationship, rights, responsibilities and obligations of all stakeholders involved in the operation.

4.7 *Interoperability means* the set of arrangements, procedures and standards that allow customers of a PSP to effect payments or transfer of funds to customers of another PSP.

4.8 *Merchant* means any person who is engaged by or on behalf of a PSP to accept payment instruments in exchange for goods and services.

4.9 *National Payment System* means a set of payment instruments, procedures and rules whereby funds are transferred among participants. The participants are entities that operate arrangements for settlement of payments among themselves, both on behalf of customers and on their own behalf.

4.10 *Outsourcing* means the contracting or sub-contracting of one or more activities, relating to the operation of a PSP, to an independent third party.

4.11 *Payment Service Provider (PSP)* means a body corporate that is authorised by the Bank to provide electronic retail payment instruments and services to customers and businesses, for the purpose of effecting payments and funds transfers. The three categories of PSPs under which a body corporate may be authorised by the Bank are:

a. *Issuers of payment instruments and services* (see **Schedule 4**), consisting of entities that:
   (i) offer payment instruments and services directly to customers;
   (ii) authorise payments; and
   (iii) guarantee payments to acquirers.
b. *Payment initiation service providers* consisting of PSPs that initiate payments at the request of customers to access value stored on payment accounts held at another PSP (see **Schedule 5**).
c. *Merchant acquirers* consisting of PSPs that are responsible for:
   (i) collecting from payees (i.e. the merchants), all the information necessary to process payments; and
   (ii) the subsequent transfer of the payment amount to payees (see **Schedule 6**).

4.12 *Suspicious Transaction* is defined in accordance with the provisions of Section 94 of the Proceeds of Crime Act to mean:

a. a complex, unusual or large business transaction carried out by a customer with the business; and

b. an unusual pattern of transactions, whether completed or not, which appear to the person to be inconsistent with the normal transactions carried out by that customer with the business.

5. Authorisation

5.1 Entities wishing to operate as PSPs are required to submit applications to the Bank to inform assessment and authorisation prior to commencement of operations. Application and prior authorisation will also be required for all agents and outsourcing arrangements.

5.2 An entity that submits an application (PSP applicant) to the Bank will be required to provide information and documents as outlined in the ERPS 2 or otherwise requested by the Bank to inform the review and authorisation processes.

5.3 PSP applicants who intend to conduct proof of concept studies and pilots, are required to submit applications to the Bank, supported by the relevant information and documents, for review and authorisation prior to commencement of operations.

5.4 PSP applicants who intend to operate closed-loop payment systems are required to submit information and documents to inform assessment and authorisation by the Bank prior to commencement of operations.

5.5 PSPs and their agents will be required to pay authorisation fees in accordance with **Schedule 1 - Authorisation Fees for the Operation of Electronic Retail Payment Services**.

5.6 PSPs shall obtain prior authorisation from the Bank for any sale, transfer, merger, acquisition or amalgamation of its interest, assets, shares or its operations, wholly or partially with any other entity.

5.7 Only PSPs, DTIs and other entities authorised by the Bank, are allowed to provide electronic retail payment instruments and services in Jamaica.

6. Capital Requirements

6.1 PSPs are required to maintain sufficient capital to support a minimum net worth of $15,000,000.00, subject to changes that the Bank may make from time to time.

6.2 Notwithstanding the provision at Section 6.1, PSPs may be required to maintain higher or lower levels of capitalisation based on the Bank's assessment of the nature and size of the PSP's operations.

7. Governance

7.1 PSPs shall establish governance arrangements, that are effective and transparent, to ensure the integrity of operations. At a minimum the governance arrangements shall include the following:

a. established processes for ensuring that shareholders, directors, managers and agents fulfill the fit and proper criteria defined by the Bank;

b. clearly defined and documented organisational arrangements to include:

i. management structure;

ii. accountabilities of significant positions in the organisational structure; and

iii. appropriate personnel management arrangements.

c. incorporation documents that provides for the conduct of electronic retail payment services business.

7.2 PSPs shall establish appropriate risk management arrangements to ensure the safety and integrity of operations. The arrangements must include at a minimum:

a. the identification of the range of risks associated with operations and the provision of services;

b. a comprehensive risk management policy, document procedures and systems to identify, measure and monitor the range of risks on an on-going basis;

c. the provision of incentives to customers or agents to manage and contain risks;

d. a liquidity management plan;

e. a capital management plan; and

f. a comprehensive internal audit function.

7.3 PSPs shall ensure that comprehensive IT audits are conducted periodically by an independent third party, with the report on the findings being presented to the Board and sub-committees of the Board to inform deliberations and decisions. The PSP will also be required to submit copies of the IT audit report and Board approved action plans to the Bank for review.

8. Operational requirements

8.1 PSPs shall establish appropriate operational arrangements to include:

a. rules, policies, procedures and agreements setting out the contractual rights, responsibilities and obligations of the PSP, third parties engaged in outsourcing arrangements, agents, merchants, customers and any other relevant stakeholders;

b. measures to ensure safety, security and operational reliability of the retail payment service, including contingency arrangements and disaster management procedures, to be applied to all relevant systems and platforms, whether internal or outsourced;

c. adequate arrangements to ensure interoperability;

d. separate, accurate and complete record of transactions and accounts for activities related to the electronic retail payment service that it provides; and

e. detailed terms and conditions for the use of the electronic retail payment service, which should be easily accessible and understood.

8.2 PSPs shall ensure that they have the necessary expertise, hardware, software, and other operating capabilities to consistently deliver reliable service, including:

a. appropriately trained staff at all levels;

b. appropriately designed system(s) that have been extensively tested;

c. effective internal control arrangements;

d. comprehensive and well documented operational and technical procedures;

e. robust clearing and settlement arrangements;

f. a robust business continuity plan including reliable fail-over and back-up systems;

g. comprehensive audit trails and the capability to provide statistical information and reports;

h. adequate accounting systems and proper reconciliation processes; and

i. complaints and dispute management arrangements, including redress mechanisms.

9. Imposition of limits

9.1 The Bank reserves the right to impose such conditions and limits on PSPs and the agents of PSPs as deemed necessary. The conditions and limits may include the extent and nature of operations, the payment instruments and services that may be offered, and the limits on the monetary values on operations and transactions.

9.2 PSPs are required to operate in accordance with the limits detailed in **Schedule 2 - Operating Limits for Payment Service Providers,** of ERPS 2. Account limits, transaction limits and daily limits that fall outside the preset levels outlined in **Schedule 2** require prior authorisation from the Bank.

10. Outsourcing

10.1 Outsourcing of managerial functions is prohibited.

10.2 PSPs who intend to outsource operational functions are required to secure prior authorisation from the Bank. In support of the request for authorisation the PSP must submit information on the identification, location, and nature of the business of the entity to which activities are to be outsourced, in addition to any other information that the Bank may request from time to time.

10.3 Authorisation for outsourcing of operational functions will be considered where the following conditions are met:

a. the outsourcing arrangement shall not result in the delegation by senior management of its responsibilities;

b. the outsourcing arrangement must not impair the internal controls;

c. the obligations of the PSP to customers shall not be altered;

d. the outsourcing arrangement must not conflict with the terms and conditions of authorisation granted by the Bank; and

e. the outsourcing arrangements will have no adverse impact on the ability of the Bank to monitor compliance with ERPS 2 or any further measures the Bank may adopt in discharging its oversight responsibilities.

10.4 PSPs shall ensure compliance with all relevant agreements and remain fully liable for the decisions and actions of entities to which activities have been outsourced.

11. Use of agents

11.1 PSPs are required to secure authorisation from the Bank prior to the engagement of agents.

11.2 PSPs in applying for authorisation to engage agents, shall provide the following information and documents to the Bank to inform the review and authorisation processes:

a. details of the criteria that will be used by the PSP for selecting and appointing agents;
b. the name, address, and other relevant information on agents;
c. documents and information on directors and persons responsible for the management of the agent to determine the fitness and propriety of all agents. The relevant documents and information include:
    i. a completed personal questionnaire;
    ii. certified photographs;
    iii. curriculum vitae;
    iv. police clearance report;
    v. Financial Investigation Division report; and
    vi. any other document requested by the Bank.
d. copies of the agency agreement, containing at a minimum clear indication of the duties and responsibilities of the agent(s), as well as, compensation arrangements; and
e. a description of the internal control mechanisms that will be used by agents in order to comply with the obligations of the PSP in relation to anti-money laundering (AML) and combating terrorist financing (CFT).

11.3 The PSP shall ensure that agents acting on its behalf inform customers of their authorisation to act as agents.

11.4 Exclusive agreements, which prohibits the agent of one issuer from serving as agent of another issuer, shall be submitted to the Bank for prior authorisation. Authorisation may not be granted where an exclusive agreement is assessed to be inconsistent with public policy objectives related to development, access and utilization of electronic retail payment services.

11.5 PSPs shall ensure compliance with all relevant agreements and remain fully liable for decisions and actions by their agents.

11.6 The Bank shall list all approved agents in a register, which will be published by the Bank at least once every six months.

12. Treatment of Merchants

12.1. PSPs are responsible for all merchant operations relating to the acceptance of payment instruments issued by the PSP.

12.2. All merchants engaged by PSPs shall be properly registered in conformity with the relevant KYC and AML guidelines. In addition, PSPs must have appropriate merchant agreement(s) to address rights, responsibilities and obligations.

13. Consumer protection, education and privacy

13.1 PSPs are required to put in place measures to promote consumer protection, education and privacy of information, to include:

a. adoption of general policies on safe operations, privacy of customers' information, reliability and quality of service, transparency of terms and conditions related to instruments and services, and prompt response to requests for refunds, inquiries and complaints;

b. establishment of appropriate dispute resolution mechanisms; and

c. provision of adequate warning statements to customers and merchants on the risk of loss arising from lost or stolen payment instruments or access devices, or fraudulent transactions.

13.2 PSPs are required to provide customers and merchants with formal agreement(s) to include details of the terms and conditions for use of the payment instrument(s) and services. The detailed terms and conditions shall include at a minimum:

a. type and description of services offered;

b. all applicable fees and charges including transaction fees, merchant fees and interchange fees;

c. all benefits to include discounts and commissions;

d. availability of customer statements;

e. procedures for reporting lost or stolen instruments and devices, and for lodging of complaints;

f. refund policy;

g. rights and responsibilities of PSP and customers;

h. termination rules;

i. redemption procedures where relevant; and

j. information on finality and irrevocability relating to the settlement of payments.

13.3 PSPs are to ensure that customers are notified, on a real-time basis, of top-ups, cash-outs and any other transaction which increases or decreases the value of funds stored in their accounts.

13.4 Consumers are required to submit written requests for account closure. All such requests must be processed and funds returned by the PSP within 3 days of the date on which requests are made.

14. Liquidity Requirement

14.1 PSPs shall maintain the following minimum liquidity requirements:

a. liquid funds of not less than three times the average maximum daily value (computed over the previous six months) of amounts required to settle customer transactions;

and

b. liquid funds of not less than six months gross operating expenses;

or

c. as an alternative or in addition to (a) and (b) above, minimum liquidity requirements determined in accordance with directives of the Bank.

15. Operating Guidelines for Payment Service Providers

15.1 PSPs shall:

a. open and operate a custodian account(s) at one or more DTI(s) regulated by the Bank and shall deposit funds collected from electronic payment service customers and funds being held on behalf of merchants into the custodian account(s). An agreement including the responsibilities outlined in Section 16 below, shall be signed by the PSP with the custodian bank;

b. submit a letter from the respective custodian bank(s) confirming the undertaking of the custodian bank to fulfill the relevant conditions and responsibilities that are outlined in Section 16 below;

c. clearly identify the set of accounts related to each custodian account maintained with one or more DTI;

d. maintain the aggregate of unused balances from sums collected from or on behalf of customers, in the custodian account/s at all times. Amounts collected from or on behalf of customers should be deposited within a maximum of one business day and held separately from other funds of the PSP;

e. report suspicious transactions of account holders based on the guidelines issued by the Designated Authority and all other relevant authorities and to strictly comply with relevant reporting requirements relating to such transactions;

f. ensure that funds in the custodian account shall only be used to effect transactions on behalf of the customer in accordance with the agreement, subject to the understanding that transactions will be limited to:

    i. settlement of obligations arising from transactions of the customer to include settlement of transactions via other payment systems;

    ii. withdrawal of funds by a customer; and

    iii. settlement of credits and debits to the custodian account to effect changes in the cumulative sum of customer account balances;

g. not use funds in the custodian account as security or collateral at any time;

h. have no claim to the funds lying in the custodian account in the case of insolvency or cessation of business of the PSPs. The Bank, or its designate, shall assume responsibility for the custodian account in the case of insolvency or cessation of business of the PSP;

i. open and maintain separate pre-funded accounts for each customer and a statement of the account shall be made available to the customer electronically or in printed form, periodically or upon request;

j. refund the remaining balance on the account to customers no later than three (3) business days from the date that a request is made. Such refunds are to be made without any additional cost other than what is necessary to complete the transaction. The account holder shall be notified with written confirmation by the PSPs, after the completion of the process for closing the account;

k. ensure strict adherence to the KYC and CDD procedures in registering customers and maintaining customer accounts;

l. monitor and supervise the activities of the account holders and merchants to ensure that they are operated for the intended purposes; and

m. submit periodic reports and provide access to the system, as and when requested by the custodian bank, in order to monitor balances and activities of account holders.

16. Responsibilities of Custodian Bank

16.1 The custodian bank shall ensure that interest earned on balances held on the custodian account is credited to a separate account for the benefit of the PSP.

16.2 The custodian bank shall:

a. provide the PSP with the ability to electronically extract transaction information on the account, as well as, request reports;

b. report the deposits in the custodian accounts as part of the deposit liabilities of the bank; and

c. cooperate with the regulatory authorities to facilitate timely payout of funds to customers from the custodian account of the PSP in the event of disruption and/or closure of the operation of the PSP.

16.3 Custodian banks shall ensure that the funds held in custodian accounts are blocked and disbursed only on the advice of the Bank in the case of the withdrawal of the authorisation granted to the PSP by the Bank.

17. Monitoring, Sanctions and Remedial Actions

17.1. The Bank shall conduct periodic evaluation and assessments of the operation and performance of PSPs.

17.2. Where operational deficiencies are identified the PSP will be required to take ameliorative actions on the directive of the Bank.

17.3. The Bank may suspend or withdraw an authorisation if the PSP:

a. fail to commence operations within 6 months after authorisation is granted; or
b. fail to comply with the terms and conditions of the authorisation; or
c. contravenes any provisions of the Guidelines or directions issued by the Bank; or
d. fails to pay annual fees within 14 days of the due date; or
e. becomes insolvent.

17.4. Where a revocation notice advising of the withdrawal of authorisation is issued by the Bank, the PSP shall be prohibited from operating with effect from the date specified in

the notice and shall comply with all the directives issue by the Bank consequent on the withdrawal of authorisation.

17.5. The Bank shall publish suspension or revocation notices issued to PSPs.

17.6. A PSP may surrender its authorisation subject to advice to the Bank at least 90 calendar days prior to the proposed date for termination of operations.

17.7. If a PSP advise of its decision to surrender its authorisation, the entity shall:

a. submit all relevant information to the Bank to facilitate the monitoring of refunds to the customers and settlement of balances due to merchants;
b. distribute the funds held in the custodian account to the account holders and settle all balances due to merchants prior to the proposed date for termination of operations, and submit reports of distribution to the Bank.

18. Other prohibitions

18.1 PSPs are responsible for ensuring that an electronic retail payment instrument shall not:

a. be issued at a premium or discount to customers;

b. be used to finance the granting of loans;

c. earn interest on unused balances; and

d. be associated, linked or used to conduct or facilitate illegal activities.

19. Reporting requirements

19.1 PSPs shall submit audited financial statements to the Bank within 90 days of the end of each financial year;

19.2 PSPs shall submit other reports as directed by the Bank, including:

a. transaction reports showing, among other information, transactions with agents and between agents, total volume and value of cash in and cash out transactions, fees collected, number of accounts opened, number of accounts closed and any other data that the Bank may from time to time consider necessary for its oversight activities;

b. complaints lodged and resolved, and the treatment of each case;

c. fee schedule and charges applied to customer accounts for use of instruments and services offered; and

d. reconciliation statements of the aggregate value of balances held for customers against balances held in the custodian account(s).

19.3 The Bank shall prepare, maintain and periodically publish a register of all PSP.

20. Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) Requirements

20.1 PSPs shall comply with the Bank's Guidance Notes on the Detection and Prevention of Money Laundering and Terrorist Financing Activities.

20.2 PSPs are required to comply with Requirements for Know Your Customer and Customer Due Diligence, as detailed in Schedule 3.

21. Pre-existing Entities

21.1 Within six (6) months of the effective date of ERPS 2, entities that are not authorised to provide electronic retail payment instruments and electronic retail payment services are required to notify the Bank of their intention to submit the necessary application for authorisation.

21.2 Failure to provide the required notification and submission of an application in accordance with Section 21.1 will result in appropriate action being taken by the Bank to protect the interest of customers and the public in general.

21.3 Entities that were previously authorised by the Bank to provide electronic retail payment services are required to ensure that they are fully compliant with the revised provisions outlined in ERPS 2 within 180 days of the date of publication.

SCHEDULE 1

AUTHORISATION FEES FOR THE OPERATION OF ELECTRONIC RETAIL PAYMENT SERVICES

1. In accordance with Section 5.5 of the Guidelines, PSPs and their agents are required to pay authorisation fees as detailed in the following table.

Authorisation Fees		
Initial Application	Payment Service Provider	$600,000
	Agent (per location)	$25,000
Annual Fee	Payment Service Provider	$600,000
	Agent (per location)	$25,000

2. No annual fee will be payable in relation to the first year of operations.

3. The Bank reserves the right to change the fees indicated in this schedule from time to time subject to a notification period of at least 90 days.

SCHEDULE 2

OPERATING LIMITS for PAYMENT SERVICE PROVIDERS

1. In accordance with Section 9.2, PSPs and their agents are required to adhere to the limits detailed in the following table.

Maximum Limits	Tier 1	Tier 2	Tier 3
Account Limits	$ 100,000	$ 200,000	$ 300,000
Daily/Transaction Limits	$ 25,000	$ 50,000	$ 75,000

2. Notwithstanding the foregoing the Bank may authorise higher Tier 3 account limits, subject to a maximum of $1,000,000.00, where the Bank is satisfied that the PSP has established the necessary risk management arrangements to mitigate the risks associated with the higher account limits and the associated higher daily/transaction limits.
3. The Bank reserves the right to change the limits outlined in this schedule subject to a notification period of at least 90 days.

SCHEDULE 3

REQUIREMENTS for KNOW YOUR CUSTOMER and CUSTOMER DUE DILIGENCE

1. In accordance with Section 20 of ERPS 2, PSPs and their agents are required to adhere to the Guidelines for know your customer (KYC) and customer due diligence (CDD) detailed in the following table.

Requirements	Tier 1 – Account Limit of $100,000	Tier 2 – Account Limit of $200,000	Tier 3 – Account Limit of $300,000 or higher limit approved by the Bank
Customer Data	Name, Gender, Date of birth, Country of birth & Nationality	Name, Gender, Date of birth, Country of birth & Nationality	Name, Gender, Date of birth, Country of birth & Nationality.
	Taxpayer Registration Number (TRN)	Taxpayer Registration Number (TRN)	Taxpayer Registration Number (TRN).
	Photo Identification issued by the Government of Jamaica (GOJ) or by an entity that is recognised by the Bank. Applicants must be physically present for identity verification excepting where an alternate verification process is authorised by the Bank.	Photo Identification issued by the Government of Jamaica (GOJ) or by an entity that is recognised by the Bank. Applicants must be physically present for identity verification excepting where an alternate verification process is authorised by the Bank.	Photo Identification issued by the Government of Jamaica (GOJ) or by an entity that is recognised by the Bank. Applicants must be physically present for identity verification excepting where an alternate verification process is authorised by the Bank.
	Copy of photo ID must be retained.	Copy of photo ID must be retained.	Copy of photo ID must be retained.
KYC and CDD Requirements		Source of funds must be verified and recorded.	Source of funds must be verified and recorded.
			Occupation or line of business must be verified and recorded.
			Proof of address must be verified and recorded.

2. Photo identification issued by the GOJ includes passport, driver's license, and any national identification cards or identification instruments that are issued by the GOJ;
3. Where a photo identification refered to at 2. above cannot be tendered, other evidence may be accepted such as:
    a. an identification card issued by an employer or, in the case of a student who is under the age of 18 years of age, a recognised academic insitution. Such ID must contain the following features:
        i. a photograph;
        ii. A signature of ID holder;
        iii. ID Number;

iv. expiry date of ID; and

v. name of relevant company or academic institution.

vi. signature of an authorised person representing the company or academic institution.

b. Where an ID that is issued by an employer is tendered the following additional documents must also be requested by the PSP to complete the identification process:

i. a birth certificate accompanied by a declaration of identification; and

ii. a letter from a person in a position of responsibility who knows the customer. Such persons include teachers, social workers, doctors, ministers of religion, justices of the peace, or attorneys-at-law.

4. Notwithstanding the foregoing the PSP is required to establish and administer appropriate risk management arrangements to ensure the integrity of the identity verification process.

5. Utilization of systems for electronic verification of identitification may be allowed by PSPs subject to authorisation by the Bank.

SCHEDULE 4

PAYMENT SERVICE PROVIDER – ISSUER OF PAYMENT INSTRUMENTS and SERVICES

1. In accordance with Section 4 of ERPS 2, an issuer of payment instruments and services are entities that:
    a. make payment instruments directly available to end users;
    b. authorize payments; and
    c. in the case of card payments, guarantee payments to the acquirers.

2. PSPs authorized as an issuer of payment instruments and services may engage in any of the following payment services:
    a. enable cash to be placed on a payment account, as well as, all the operations required for operating a payment account;
    b. enable cash withdrawals from a payment account, as well as, all the operations required for operating a payment account;
    c. execute payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider;
    d. issue payment instruments and/or acquire payment transactions;
    e. money remittance; and
    f. payment initiation services.

3. All provisions of ERPS 2 must be adhered to by issuers of payment instruments and services.

SCHEDULE 5

PAYMENT SERVICE PROVIDER – PAYMENT INITIATION SERVICE PROVIDER

1. In accordance with Section 4 of ERPS 2, payment initiation service providers are entities offering a service to initiate a payment at the request of the end user, accessing value stored on payment accounts held at another institution offering payment services.

2. PSPs that are authorised as payment initiation service providers may engage in the following functions on behalf of payment service users:
    a. request payment service provider of choice and receive instructions;
    b. initiate payment requests;
    c. send payment initiation request to payment service provider;
    d. receive payment initiation response from payment service provider;
        i. confirm execution or rejection of payment initiation request to payment service users via notifications;
    e. request payment report from payment service providers; and
    f. send payment initiation status to receiver of the payment.

3. Payment Initiation Service Providers must meet the following requirements:
    a. maintain appropriate capital for the business of payment initiation;
    b. maintain contracts with payment service users and payment service providers;
    c. protect sensitive data of payment service users throughout the payment initiation value chain;
    d. apply strong customer authentication methods;
    e. provide reports as requested by the Bank; and
    f. comply with applicable provisions within the Guidelines.

SCHEDULE 6
PAYMENT SERVICE PROVIDER – MERCHANT ACQUIRER

1. In accordance with Section 4 of the Guidelines, merchant acquirers are entities responsible for:
    a. collecting from the payee (i.e. the merchant) all the information necessary to process the payment; and
    b. the subsequent transfer of the payment amount to the payee.

2. PSPs authorized as a merchant acquirer may engage in the following functions:
    a. receive payment data or requests from the merchant;
    b. send payment data or request to payment service provider for authentication;
    c. receive payment confirmation response from payment service provider;
    d. receive funds transfer from payment service provider;
    e. send confirmation or rejection status request to merchant;
    f. send funds to merchant account; and
    g. provide statement on merchant transactions.

3. Merchant Acquirers must meet the following requirements:
    a. build and maintain a secure network;
    b. protect customer data;
       implement strong access control measures;
    c. regularly monitor and test networks; and
    d. maintain a policy that addresses information security.