Royal Monetary Authority of Bhutan

Payment Aggregators and Payment Gateways Guideline 2020

In exercise of the powers conferred by Payment and Settlement Systems Rules and Regulations 2018, the RMA hereby issues this Guideline for the effective operations of Payment Aggregator and Payment Gateway in the country.

SECTION I: PRELIMINARY

1. Short Title and Commencement

   This Guideline Shall:

   a) Be cited as the Payment Aggregators and Payment Gateways Guidelines 2020;

   b) Come into force with effect from October 2020.

2. Applicability

   a)   The guideline shall be applicable to Payment Aggregators (PAs). PAs shall also adopt the technology-related recommendations provided in Annex I. As a measure of good practice, the Payment Gateways (PGs) may adhere to these baseline technology-related recommendations;

   b)   Domestic leg of import and export related payments facilitated by PAs shall also govern by this guideline;

   c)   The guidelines are not applicable to:

      i.   Intermediaries who facilitate delivery of goods / services immediately / simultaneously (e.g. travel tickets / movie tickets, etc.) on the completion of payment by the customer i.e., where the delivery is linked to completion of corresponding payment;

      ii. Cash on Delivery (CoD) e-commerce model;

      iii. e-commerce marketplaces collecting payments for various merchants for transactions in respect of goods and services sold on their platform;

      iv. Other bilateral arrangements of merchants with the aggregators to consolidate and make payments to vendors, agents, etc.

3. Definitions

   a)   For the purpose of this guideline, the PAs and PGs are defined as under:

      i.   Payment Aggregators: PAs are entities that facilitate e-commerce sites and merchants to accept various payment instruments from the customers for completion of their payment obligations without the need for merchants to create a separate payment integration system of their own. PAs facilitate merchants to connect with acquirers. In the process, they receive payments from customers, pool and transfer them on to the merchants after a time period;

      ii. Payment Gateways: PGs are entities that provide technology infrastructure to route and facilitate processing of an online payment transaction without any involvement in handling of funds.

   b)   In the processing of an online transaction the following timelines are involved:

      i.   'Tp' – date of charge / debit to the customer's account against the purchase of goods / services;

ii. 'Ts' – date of intimation by the merchant to the intermediary about shipment of goods;

iii. 'Td' – date of confirmation by the merchant to the intermediary about delivery of goods to the customer;

iv. 'Tr' – date of expiry of refund period as fixed by the merchant.

c) Other terminology used in this guideline will have same meaning and definition to the Payment and Settlement Systems Rules and Regulations 2018.

4. Purpose
The primary purpose of this guideline is to set certain minimum standard and procedures to ensure smooth, secure and effective operation and functioning of Payment Aggregators and Payment Gateways in the country.

5. Supersession
This guideline shall supersede any Guideline, Circulars or Notifications that are inconsistent with this Guideline.

6. Interpretation
The authority for the final interpretation of any provision of this guideline shall vest with the RMA which, if warranted, may issue such instruction and clarification from time to time as may be necessary to give effect and implement this guideline.

7. Amendment
The amendment relating to addition, changes or repeal of any provisions of this guideline shall be made by the Executive Committee based on the recommendation of the Management.

SECTION II: AUTHORISATION

8. Authorisation:
a) All Authorized Bank, licensed Payment Systems Operator and any other Payment Systems Provider authorized by RMA desirous of becoming PAs providing a payment aggregator service, shall apply to the Authority for an authorisation prior to the commencement of its operations;

b) Entities seeking authorisation as PA from the RMA, shall apply in Form A to the Department of Payment and Settlement Systems (DPSS), RMA.

9. Authorisation Criteria:
a) The Authority shall not grant an authorisation if the following requirements are not met:
a) PAs shall be a company incorporated under the Companies Act 2016;

b) All essential activities of the payment aggregator service are to be carried out in the country;

c) The overall organization and structure, security policies of the proposed PAs are adequate to safeguard the integrity, authenticity, and confidentiality of data and there is adequate business continuity, disaster recovery plan;

d) The Board of directors adequately reflects the balance of interest represented by the PAs, in particular that the company will hold funds in trust on behalf of merchant and customer.

e) The applicant or any of its significant owners have been convicted of an offence involving a financial transaction in any jurisdiction within the past ten (10) years;

f) The applicant fails to respond to a request from the Authority for additional information within ten (10) days of a third request for the same information;

g) The documents submitted are false, incomplete, deceptive or misleading;

h) Any applicant for PAs whose application has been refused or suspended, restricted or revoked may, within thirty (30) days from the date on which the order is communicated to him or her, appeal against the decision;

10. Authorisation conditions. The Authority may at any time make the authorisation conditional upon any terms or conditions which the Authority deems appropriate for the safety and efficiency of the PAs and the financial system at large.

11. Authorization and issuance of additional PAs instruments: Where the Authority is of the opinion that:

a) Payment aggregator is of widespread use as a means of making payment and plays significant role in development of Bhutan's payment system;

b) It is necessary to protect the interest of the public by ensuring the integrity, security and reliability of the payment instrument as a designated payment instrument;

c) No PAs shall introduce any new payment instrument or service without prior written approval of the Authority;

d) The Authority may set out standards for payment instruments and services and stipulate transition time frame for the existing instruments or services, if necessary.

e) The design, security and operational risk management features if necessary, shall be decided by the Authority;

f) The Authority may in granting authorization require all or any of the documents submitted to be modified and altered as it may deem necessary;

g) Impose such restriction, limitations or conditions as it may deem fit.

12. Power to approve changes in a system.

a) No PAs shall cause any change in the system it operates which would substantially affect the structure or the operation of the system without:

   i. The prior written approval of the Authority; and

    ii.   Giving notice of not less than thirty (30) days to the system participants after obtaining approval of the Authority.

b) Notwithstanding section, the Authority may permit a PAs to make any quick change in a system without giving notice to the system participants or require a system to give notice for a period longer than thirty (30) days, if it deems this is the interest of monetary policy of the country or in the public interest.

c) Where the Authority has any objection to the proposed change for any reason, it shall notify such objection to the PAs within ten (10) working days of receipt of the intimation for the proposed changes. In technically complex cases, the Authority may extend this deadline by ten (10) additional working days, by reasoned decision.

13. Prohibition of Issuance of payment aggregator service

The Authority may, in written order, reject the issuance or using any PAs service if, in its reasoned opinion:

a)   The issuance or use of the payment instrument violates or contravened any law, rules and regulation or order of the Authority;

b)   Failed to commence the operation of payment instrument within six (6) months after the approval/ authorization was granted;

c)   Ceased issuing the payment instrument for more than thirty (30) days;

d)   The authorization for payment instrument has been obtained through incomplete, misleading or false information or any other irregular or illegal means;

e)   The Payment Aggregator commits an act of bankruptcy;

f)   Is no longer to public's interest, no longer represents the interests of the participants; endangers the stability of the financial system in the country; or

g)   There exists any other ground which in the opinion of the Authority warrants variation or revocation.

Section III: GOVERNANCE

14. Governance
   a) The Directors and the Management of the proposed entity are fit and proper;
   b) PAs shall be professionally managed. The promoters of the entity shall satisfy the fit and proper criteria prescribed by RMA;
   c) The directors/CEO of the applicant entity shall submit a declaration in the enclosed format;
   d) RMA shall also check 'fit and proper' status of the applicant entity and the management by obtaining inputs from other regulators, government departments, etc., as deemed fit;
   e) Applications of those entities not meeting the eligibility criteria, or those which are incomplete / not in the prescribed form with all details, shall be returned;

f) The overall organization and structure of the proposed entity is adequate for its operations and includes robust procedures for the management of its liquidity and credit risk; data protection; contingency and disaster recovery;

g) Any takeover or acquisition of control or change in management of a non-bank PA shall be communicated by way of a letter to the Director, Department of Payment and Settlement Systems (DPSS) within 15 days with complete details, including 'Declaration and Undertaking' by each of the new directors, if any. RMA shall examine the 'fit and proper' status of the management and, if required, may place suitable restrictions on such changes;

h) Agreements between PAs, merchants, acquiring banks, and all other stake holders shall clearly delineate the roles and responsibilities of the involved parties in sorting / handling complaints, refund / failed transactions, return policy, customer grievance redressal (including turnaround time for resolving queries), dispute resolution mechanism, reconciliation, etc.;

i) PAs shall disclose comprehensive information regarding merchant policies, customer grievances, privacy policy and other terms and conditions on the website and / or their mobile application;

j) PAs shall have a Board approved policy for disposal of complaints / dispute resolution mechanism / time-lines for processing refunds, etc., in such a manner that the RMA instructions on Turn Around Time (TAT) for resolution of failed transactions are adequately taken care of. Any future instructions in this regard shall also be adhered to by PAs;

k) PAs shall appoint an Officer responsible for regulatory and customer grievance handling functions. PAs shall prominently display details of the officer on their website or any other platform.

15. Safeguards against Money Laundering (KYC / AML / CFT) Provisions
   a) Ensure it complies with the applicable provisions of the Anti-Money Laundering and Combating the Financing of Terrorism Rules and Regulations 2018 and amendment thereof;
   b) The Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) guidelines issued by the RMA, shall be applicable;
   c) Abide to the provision of the Payment and Settlement Systems Rules and Regulations, 2018, Payment System Oversight Framework, BIPS procedural guideline and any other applicable guideline, rules and regulations.

SECTION IV: MERCHANT ON-BOARDING AND SETTLEMENT ACCOUNT

16. Merchant On-boarding

   a) PAs shall have a Board approved policy for merchant on-boarding;
   b) PAs shall ensure that such merchants do not have any mala fide intention of duping customers, do not sell fake / counterfeit / prohibited products, etc. The merchant's website shall clearly indicate the terms and conditions of the service and time-line for processing returns and refunds;
   c) PAs shall be responsible to check Payment Card Industry-Data Security Standard (PCI-DSS) and Payment Application-Data Security Standard (PA-DSS) compliance of the infrastructure of the merchants on-boarded;
   d) Merchant site shall not save customer card and such related data. A security audit of the merchant may be carried out to check compliance, as and when required;
   e) Agreement with merchant shall have provision for security / privacy of customer data;
   f) PAs agreement with merchants shall include compliance to PA-DSS and incident reporting obligations. The PAs shall obtain periodic security assessment reports either based on the risk assessment (large or small merchants) and / or at the time of renewal of contracts.

17. Settlement and Escrow Account Management

   a) PAs shall maintain the amount collected by them in an escrow account with any commercial bank;
   b) Escrow account balance shall be maintained with only one commercial bank at any point of time. In case there is a need to shift the escrow account from one bank to another, the same shall be effected in a time-bound manner without impacting the payment cycle to the merchants under advise to RMA;
   c) Amounts deducted from the customer's account shall be remitted to the escrow account maintaining bank on $Tp+0$ / $Tp+1$ basis. The same rules shall apply to the non-bank entities where wallets are used as a payment instrument;
   d) Final settlement with the merchant by the PA shall be effected as under:
      i. Where PA is responsible for delivery of goods / services the payment to the merchant shall be not later than on $Ts + 1$ basis;
      ii. Where merchant is responsible for delivery, the payment to the merchant shall be not later than on $Td + 1$ basis;
      iii. Where the agreement with the merchant provides for keeping the amount by the PA till expiry of refund period, the payment to the merchant shall be not later than on $Tr + 1$ basis.
   e) Credits towards reversed transactions (where funds are received by PA) and refund transactions shall be routed back through the escrow account unless as

per contract the refund is directly managed by the merchant and the customer has been made aware of the same;

f)   At the end of the day, the amount in escrow account shall not be less than the amount already collected from customer as per 'Tp' or the amount due to the merchant;

g)   PAs shall be permitted to pre-fund the escrow account with own / merchant's funds. However, in the latter scenario, merchant's beneficial interest shall be created on the pre-funded portion;

h)   Permitted credits / debits to the escrow account shall be as set out below:

Credits

     i.   Payment from various customers towards purchase of goods / services.

     ii.   Pre-funding by merchants / PAs;

     iii.   Transfer representing refunds for failed / disputed / returned / cancelled transactions;

     iv.   Payment received for onward transfer to merchants under promotional activities, incentives, cash-backs etc.

Debits

     i.   Payment to various merchants / service providers;

     ii.   Payment to any other account on specific directions from the merchant;

     iii.   Transfer representing refunds for failed / disputed transactions;

     iv.   Payment of commission to the intermediaries. This amount shall be at pre-determined rates / frequency;

     v.   Payment of amount received under promotional activities, incentives, cash-backs, etc.

i)   For banks, the outstanding balance in the escrow account shall be part of the posit liability;

j)   The entity and the escrow account banker shall be responsible for compliance with RMA instructions issued from time to time. The decision of RMA in this regard shall be final and binding;

k)   Settlement of funds with merchants shall not be co-mingled with other business, if any, handled by the PA;

l)   PAs shall submit the list of merchants acquired by them to the bank where they are maintaining the escrow account and update the same from time to time. The bank shall ensure that payments are made only to eligible merchants / purposes. There shall be an exclusive clause in the agreement signed between the PA and the bank maintaining escrow account towards usage of balance in escrow account only for the purposes mentioned above.

SECTION V: DISPUTE MANAGEMENT FRAMEWORK

18. Customer Grievance Redressal and Dispute Management Framework

   a) PAs shall put in place a formal, publicly disclosed customer grievance redressal and dispute management framework, including designating an officer to handle the customer complaints / grievances and the escalation matrix. The complaint facility, if made available on website / mobile, shall be clearly and easily accessible;

   b) PAs shall appoint an Officer responsible for regulatory and customer grievance handling functions. Details of the officer for customer grievance shall be prominently displayed on their website;

   c) PAs shall have a dispute resolution mechanism binding on all the participants which shall contain transaction life cycle, detailed explanation of types of disputes, process of dealing with them, compliance, responsibilities of all the parties, documentation, reason codes, procedure for addressing the grievance, turn-around-time for each stage, etc.

19. Security, Fraud Prevention and Risk Management Framework

   a) A strong risk management system is necessary to meet the challenges of fraud and ensure customer protection. PAs shall put in place adequate information and data security infrastructure and systems for prevention and detection of frauds.

   b) PAs shall put in place Board approved information security policy for the safety and security of the payment systems operated by them and implement security measures in accordance with this policy to mitigate identified risks.

   c) Baseline technology-related recommendations for adoption by the PAs are provided in Annex I. The PGs may also adopt them as best practices.

   d) PAs shall establish a mechanism for monitoring, handling and follow-up of cyber security incidents and breaches. The same shall be reported immediately to the RMA.

   e) PAs shall not store the customer card credentials within their database or the server accessed by the merchant. They shall comply with data storage requirements as applicable.

   f) PAs shall ensure that the extant instructions with regard to Merchant Discount Rate (MDR) are followed, if any. Information on other charges such as convenience fee, handling fee, etc., if any, being levied shall also be displayed upfront by the PA.

   g) PAs shall not place limits on transaction amount for a particular payment mode. The responsibility therefor shall lie with the issuing bank / entity; for instance, the card issuing bank shall be responsible for placing amount limits on cards issued by it based on the customer's credit worthiness, spending nature, profile, etc.

   h) PAs shall not give an option for ATM PIN as a factor of authentication for card-not-present transactions.

   i) All refunds shall be made to the original method of payment unless specifically agreed by the customer to credit to an alternate mode. Other Recommendations

   j) All refunds shall be made to original method of payment unless specifically agreed by the customer to credit an alternate mode.

SECTION VI: OVERSIGHT AND REPORT

20. Oversight and supervision.
   a)   The Authority shall have powers to oversight and supervision of authorised PAs, and participants, as it deems necessary to ensure the safety and soundness of such PAs scheme;
   b)   The Authority shall conduct onsite and offsite supervision of the operations of authorised PAs, and any third parties to which part of services have been outsourced as per the Payment and Settlement Systems Oversight Framework;
   c)   The Authority may require all PAs with reporting requirements on their activities from time to time to oversee and for statistical purposes;
   d)   Notwithstanding anything contained in sections of the FSA, the Authority shall be allowed access to review the IT system and database of the PAs. Whenever the circumstances warrant, such access must extend to the agents, partners, service providers or outsourced entities of the PAs in view of their participation in the business.

21. Reports
   a)   The Authority may call for, or access, from PAs, its merchant, agents and distributors, such returns or documents or information relating to the business as it may require from time to time;
   b)   Without prejudice to the generality of section, the Authority may require any PAs to provide, in the form of a periodic report or otherwise information relating to operation and the pricing of, or other form of consideration;
   c)   Report volume and value of transactions to the Department of Payment and Settlement System, RMA on monthly basis or as an when required by the Authority.

Annex I

Baseline Technology-related Recommendations

Indicative baseline technology-related recommendations for adoption by the PAs (mandatory) and PGs (recommended) are:

1. Security-related Recommendations

The requirements for the entities in respect of IT systems and security are presented below:

a)   Information Security Governance: The entities at a minimum shall carry out comprehensive security risk assessment of their people, IT, business process environment, etc., to identify risk exposures with remedial measures and residual risks. These can be an internal security audit or an annual security audit by an independent security auditor. Reports on risk assessment, security compliance posture, security audit reports and security incidents shall be presented to the Board.

b)   Data Security Standards: Data security standards and best practices like PCI-DSS, PA-DSS, latest encryption standards, transport channel security, etc., shall be implemented.

c)   Security Incident Reporting: The entities shall report security incidents / card holder data breaches to RMA. Cyber security incident reports with root cause analysis and preventive actions undertaken shall be submitted to RMA.

d)   Merchant Onboarding: The entities shall undertake comprehensive security assessment during merchant onboarding process to ensure these minimal baseline security controls are adhered to by the merchants.

e)   Cyber Security Audit and Reports: The entities shall carry out and submit to the IT Committee quarterly internal and annual external audit reports; bi-annual Vulnerability Assessment / Penetration Test (VAPT) reports; PCI-DSS including Attestation of Compliance (AOC) and Report of Compliance (ROC) compliance report with observations noted if any including corrective / preventive actions planned with action closure date; inventory of applications which store or process or transmit customer sensitive data; PA-DSS compliance status of payment applications which stores or processes card holder data.

f)   Information Security: Board approved information security policy shall be reviewed at least annually. The policy shall consider aspects like: alignment with business objectives; the objectives, scope, ownership and responsibility for the policy; information security organisational structure; information security roles and responsibilities; maintenance of asset inventory and registers; data classification; authorisation; exceptions; knowledge and skill sets required; periodic training and continuous professional education; compliance review and penal measures for non-compliance of policies.

g) IT Governance: An IT policy shall be framed for regular management of IT functions and ensure that detailed documentation in terms of procedures and guidelines exists and are implemented. The Board level IT Governance framework shall have

    i.   Involvement of Board: The major role of the Board / Top Management shall involve approving information security policies, establishing necessary organisational processes / functions for information security and providing necessary resources.

    ii.   IT Steering Committee: An IT Steering Committee shall be created with representations from various business functions as appropriate. The Committee shall assist the Executive Management in implementation of the IT strategy approved by the Board. It shall have well defined objectives and actions.

    iii.   Enterprise Information Model: The entities shall establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with board approved IT strategy. The model shall facilitate optimal creation, use and sharing of information by a business, in a way that it maintains integrity, and is flexible, functional, timely, secure and resilient to failure.

    iv.   Cyber Crisis Management Plan: The entities shall prepare a comprehensive Cyber Crisis Management Plan approved by the IT strategic committee and shall include components such as Detection, Containment, Response and Recovery.

h) Enterprise Data Dictionary: The entities shall maintain an "enterprise data dictionary" incorporating the organisation's data syntax rules. This shall enable sharing of data across applications and systems, promote a common understanding of data across IT and business users and prevent creation of incompatible data elements.

i) Risk Assessment: The risk assessment shall, for each asset within its scope, identify the threat / vulnerability combinations and likelihood of impact on confidentiality, availability or integrity of that asset – from a business, compliance and / or contractual perspective.

j) Access to Application: There shall be documented standards / procedures for administering an application system, which are approved by the application owner and kept up-to-date. Access to the application shall be based on the principle of least privilege and "need to know" commensurate with the job responsibilities.

k) Competency of Staff: Requirements for trained resources with requisite skill sets for the IT function need to be understood and assessed appropriately with a periodic assessment of the training requirements for human resources.

l) Vendor Risk Management: The Service Level Agreements (SLAs) for technology support, including BCP-DR and data management shall categorically include clauses permitting regulatory access to these set-ups.

m) Maturity and Roadmap: The entities shall consider assessing their IT maturity level, based on well-known international standards, design an action plan and implement the plan to reach the target maturity level.

n) Cryptographic Requirement: The entities shall select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies, reputable security vendors or government agencies.

o) Forensic Readiness: All security events from the entities infrastructure including but not limited to application, servers, middleware, endpoint, network, authentication events, database, web services, cryptographic events and log files shall be collected, investigated and analysed for proactive identification of security alerts.

p) Data Sovereignty: The entities shall take preventive measures to ensure storing data in infrastructure that do not belong to external jurisdictions. Appropriate controls shall be considered to prevent unauthorised access to the data.

q) Data Security in Outsourcing: There shall be an outsourcing agreement providing 'right to audit' clause to enable the entities / their appointed agencies and regulators to conduct security audits. Alternatively, third parties shall submit annual independent security audit reports to the entities.

r) Payment Application Security: Payment applications shall be developed as per PA-DSS guidelines and complied with as required. The entities shall review PCI-DSS compliance status as part of merchant onboarding process.

Form A: APPLICATION FOR AUTHORISATION TO SET UP A PAYMENT AGGREGATOR

<div align="right">Date:</div>

The Director

Department of Payment & Settlement Systems

Royal Monetary Authority of Bhutan,

Thimphu

Subject: Application to establish a Payment Aggregator Service in Bhutan

Dear Sir/Madam,

In accordance with the Payment and Settlement Systems Rules and Regulation, 2018 and Payment Aggregators and Payment Gateway Guideline 2020, we would like to apply for a license and also the Authorisation to establish a Payment Aggregator service in Bhutan and agree to abide by the Royal Monetary Authority of Bhutan Act, 2010 and the above mentioned Rules and Regulations as amended from time to time. An electronic funds transfer transaction (Reference) No……….. for an amount of …………. (Ngultrum …………. only) as non-refundable application fees is enclosed with the application. We also declare that RMA will not be held responsible for any service related issues with regards to the operation of PAs.

Yours sincerely,

Signature:

Name:

Address:

Telephone number:

Fax number:

Email:

INSTRUCTIONS

- *Application must be made in the prescribed Form A only. Wherever space is insufficient, information may be furnished in a separate sheet;*
- *Application along with enclosures duly completed should be page numbered and submitted to the Payment and Settlement Systems Department, Royal Monetary Authority of Bhutan;*
- *Application must be signed by an official who has the authority to do so such as, Chairman, Managing Director, Chief Executive Officer, or the proprietor;*
- *Application must bear common seal of the firm/company;*

1. Name of the applicant ……………………………………………………..
   i.   Name of the company: …………………………………………….
   ii.   Head Office: …………………………………………………
   iii. Address: ……………………………………………………
   iv.   Phone No: ……………………………………………………
   v.   Fax No: …………………………………………………
   vi.   Email: ……………………………………………………………

2. Please indicate the payment services the applicant intends to provide:
   i.   …………………………..….
   ii.   ………………………..….
   iii. ………………………….
   iv.   ………………………….

3. Internal Control System

Please provide us each copy of the following manuals/procedures pertaining to the payment services offered:

   i.   Operational manual
   ii.   IT security and controls guidelines
   iii. Internal control procedures, risk management and risk control procedures, Customer protection policy
   iv.   KYC and CDD procedures
   v.   Merchant due diligence manual

4. Plans for appointing stakeholders for the payment aggregator services, including the services to be provided by each stakeholder.
   ……………………………………………………………………………………………
   ……………………………………………………………………………………………
   ………………………………………………

5. The proposed capital structure of the Payment Institution:
i.   Authorized capital……………………………………………………
ii.   Issued capital…………………………………………………………..
iii.   Paid-up capital……………………………………………………………………
iv.   Source of capital……………………………………………………..

6. Details of the applicant: Provide the following key aspects of the company:
i.   Name: …………………………………………………
ii.   Date of Registration:…………………………………….
iii.   Registration number: …………………………………
iv.   Place of registration: …………………………………
v.   Type of business: …………………………………
vi.   Number of shares in proposed company:………………………

7. To submit the biographical report (details of each applicant, director(s), and key personnel of the proposed PAs in the form prescribed by RMA).

8. Additional information required to be submitted along with the application:
i.   Trade/Business License issued under Companies Act, 2016;
ii.   Feasibility report:
        a. Marco economic background/environment of Bhutan
        b. Financial system and structure
        c. SWOT analysis
        d. Survival and growth strategies/justification
        e. Business plan
9. The Payment Institution is required to submit a comprehensive and detailed business plan that consists of at least the following:
i.   Executive summary;
ii.   Mission statement;
iii.   Company overview – group structure, proposed board of directors, management team, staffing;
iv.   Product strategy- all product lines;
v.   Marketing plan, strategy, sales strategy, distribution channels and break –even analysis;
vi.   Financial plan
vii.   Latest three year audited and certified financial statements of the applicant in case of a legal entity;

BIOGRAPHICAL REPORT OF CEO/DIRECTOR and KEY POST HOLDERS

1. Personal Details.

a. Name	
b. Date of Birth	
c. Nationality	
d. Citizenship ID No.	
e. Passport No. (Non-Bhutanese)	

2. Contact Information

a. Telephone No	
b. Mobile No.	
c. Fax No.	
d. E-mail	

3. Present Position.

a. Name and Address of the Firm	
b. Nature of Business	
c. Telephone No	

4. Marital Status.

Single	Married	Divorced
If married, Spouse's Name and Citizenship ID No.		

5. Dependents.

Name	Relationship	Date of Birth (dd/mm/yyyy)

6. Family History.

Relationship	Name	Date of Birth	Occupation	Email Address	Mobile No.
Father					
Mother					

7. Education.

Name & Address of University	Years of Attendance	Major Area of Study	Degree/Certificate Granted	Date Awarded

8. Employment Record (Pertaining to previous 5 years). Use additional sheets, if necessary, and account for all gaps in employment.

Position held/ Department	Main responsibilities	Organization	Country	Duration

9. Status of the proposed appointment. Please tick relevant box

Initial Appointment	Independent Director	Non-Independent Director
Re-appointment		

10. Do you have a license to practice any profession? Yes   No

If yes, please give details.

a. Nature of License	
b. Date of Issue	
c. License/Registration No.	
d. Licensing Agency and Address	

11. (a) If self-employed, describe each enterprise, including the name, address, license number, your percentage of ownership and the type of business which you own or control. (Control means ownership of 10% or more of the stock or ability to effectively control the management of the corporation or other entity).

(b) List names, addresses and percentage of control and/or ownership of other incorporators, partners, directors, or officers of the entity or corporation referred to above.

Are you employed in any professional capacity, or do you perform any services for or have any business connections with any institution which is subject to the supervision of the Royal Monetary Authority of Bhutan, or any other authority of the Royal Government of Bhutan? If "Yes", indicate the name of the institution, address and nature of your work.	Yes No

12.

Have you had, or do you now have, any financial interest, direct or indirect, in any financial institution in Bhutan If "Yes", give the name of the institution, address and nature of the financial interest.	Yes No

13. Please tick whichever is relevant for the following questions below.

Do you have more than 5 years experience in banking, finance, accounting & information technology.	Yes	No	N/A
Were you declared insolvent and adjudicated bankrupt	Yes	No	N/A
Were you convicted by a court in any criminal offense or has been involved in any fraud/forgery, financial crime or other illegal activities	Yes	No	N/A

14. Practicing accountants may be appointed as directors provided they are not employed or are not partners in an accounting firm, which has been engaged to conduct audit or consultancy work for that particular financial institution.

15. Are you a practicing accountant/consultant? Yes No
    If "yes", in what capacity?

16. Are you affiliated to any political party? Yes No
    If "yes", in what capacity?

17. Answer "Yes" or "No" to any of the questions below if they apply to you as an individual, or a partner, director or officer of a corporation except for minor traffic violations.

a. Are any arrests, indictments, criminal information or other criminal proceedings now pending against you?	Yes No
b. Were you ever convicted for any violations of the law?	Yes No

c. Have you or has any partnership of which you were a CEO or a major owner (more than or equal to 10% of the capital of the company) ever been liquidated or judged bankrupt?	Yes No
d. Has any business of which you were a director, officer, partner or major shareholder (10% or more of the voting shares) defaulted on his/her loan repayment?	Yes No
e. Has any enterprise in which you were a partner, director or officer been the subject of criminal indictment or other criminal proceedings?	Yes No

DECLARATION

I certify and I am aware that, it is an offence under the Royal Monetary Authority Act of Bhutan 2010 and the Payment and Settlement Systems Rules and Regulation, 2018 to provide the Authority any information which is false or misleading. I certify that the information given in the form above and accompanying documents is complete and accurate to the best of my knowledge, information and belief and that there are no other facts relevant to this application of which the Authority should be aware. I also undertake that as long as I continue to be a Director/CEO/Key post holder, I will notify the Authority of any material changes to, or affecting the completeness or accuracy of, the information given above as soon as possible, but in any event no later than 10 days from the day the changes come to my attention. Further, I would like to pledge that as long as I continue to be a Director CEO/Key post holder of the company, I will not violate any laws and regulations of the Authority.

Name…………………………………………….

Position held……………………………………..

Signed…………………………………………….

(Affix legal stamp)

Date……………………………………………...

Witness

Name…………………………………………………….

Citizenship ID No (please attest a copy)…………………………………………

Address: …………………………………………………………………….

Occupation: …………………………………………………………………

Telephone number: ……………………………………………………………….

Email: …………………………………………………………………….
Signed………………………………………………………………………

Royal Monetary Authority of Bhutan

Thimphu

CERTIFICATE OF LICENSE NO:

In exercise of the powers conferred on the RMA by Section 184 of the Royal Monetary Authority of Bhutan Act, 2010 read with Clause (c) of Section 8 and Clauses (c), (h) and (l) of Section 9, Payment & Settlement Systems Rules and Regulation, 2018 and Rules and Regulation of Payment Aggregators and Payment Gateway 2020 thereof .... is hereby issued with Authorisation to establish Payment System Aggregator and operate payment aggregator service, with effect from … … ……, subject to compliance with the terms and conditions given on the reverse of this Certificate.

At Thimphu on this .... day of...............

(Signature)

RMA Seal

(Designation of the officer)

Terms and Conditions*

1. The certificate of license or a certified copy thereof shall be displayed at the main premises of the Payment Aggregator and its other offices.
2. The Payment Aggregator Service Provider shall adhere to the provisions of the Rules and Regulation of Payment Aggregator and Payment Gateway 2020, Payment and Settlement Systems Rules and Regulations, 2018, Payment Aggregator and Payment Gateway Guideline 2020 and the directions/guidelines issued by the Royal Monetary Authority of Bhutan from time to time.
3. (Any other conditions as may be specified)