Enterslice

RBI Guidelines

for

Payment Aggregators & Payment Gateways

Good Governance for Digital India

About

Enterslice

We are an Award Winning Legal and CPA Information Technology Enabled Services (ITES) concern.

We at Enterslice are committed to provide assistance to the entrepreneurs in legal registration procedures and in managing their business globally.

Be it a startup business or a well established concern, our dedicated professionals are resolved to provide bespoke solutions as regards business registration and legal compliance.

Our bevy of competent business advisers help to trace, decode and execute key business growth strategies.

Our wide range of legal & business registration services includes GST Registration, Company Registration, ITR Filing, ESI & PF Registration, NBFC & Microfinance Company Registration, FEMA Advisory and much more.

Our Core Operations:

- **Business solutions**
- **Fin-tech Solutions**
- **ITES Systems**
- **LegalTech Solutions**
- **Management Advisory**
- **HR Services**
- **FEMA Advisory**

From a strategy review of the Business development to the complete hands-on implementation, Enterslice Advisory can be truly your legal companion to grow your venture to a level further.

Contents

New RBI Guidelines

For PAs & PGs

What are the recent RBI Guidelines for PAs & PGs?

The Reserve Bank of India (RBI) had recently rolled out new guidelines in order to regulate the activities of the online Payment Aggregators (PAs) and to implement baseline technology-related recommendations for Payment Gateways (PGs). The Guidelines on Regulation of Payment Aggregators and Payment Gateways were issued on 17th March 2020.

Before we go into the depth of these guidelines, we must first get an idea about the Payment Aggregators and Payment Gateways.

Payment Aggregators & Payment Gateways

As we know that these days the use of Online Payment modes for goods and services like bill payments and online shopping etc. is being encouraged throughout the nation. This is due to the impetus of the Indian government for a cashless economy based on digital transactions. As a result, there has been increased facilitation by banks as well as the prepaid payment instrument (PPI) issuers for the use of electronic modes for payments to merchants.

This process usually involves the role of certain intermediaries like payment aggregators and payment gateway service providers. These entities create a link between the customers and the merchants and facilitate digital (cashless) transactions between them. Besides, many E-Commerce (Amazon Pay) and M-Commerce service providers (JioPay, Apple Pay, etc) have also been providing such online platforms for digital payments. However, we will be discussing about the PAs and PGs in detail. Before that, we must get familiar with the concept of PA and PG.

Definition of
Payment Aggregators

As per the Definition of Reserve Bank of India, a Payment Aggregator (PA) is an entity that:

- Facilitate e-commerce *sites & merchants* to accept various
- *Payment instruments* from their customers for fulfilling their payment obligations,
- Without the need for merchants to maintain their s*eparate payment integration* system.

Some examples of PA

PayU **BillDesk** *All your payments. Single location* **ezetap**

Instamojo **CC Avenue**

From above, we understand that PAs are the cloud-based service providers that enable the merchants to connect with acquirer banks, which process online payment on the merchant's behalf. In this entire process, PA receives payments from different users. Thereby they pool all payments and then transfer them directly onto the merchants after certain period of time.

Some examples include- Instamojo, Billdesk, PayUMoney etc.

Definition of

Payment Gateways

As per the Definition of Reserve Bank of India, a a Payment Gateway (PGs) are those entities that:

- *Provide technology* infrastructure for
- *Routing and facilitating* the procedure of an online transaction without any involvement of handling funds.

Some examples of PA

In simple words, a Payment Gateway is basically a cloud-based software or application that enables the e-commerce businesses to carry out online transactions through the website/mobile-app. These portals simply allow the online payment via credit/debit cards, net-banking, e-wallets and UPI.

Some examples include- BHIM, PayTm, Phonepe, Mobikwik, PayPal etc.

Importantly, here is the key to the timelines involved in the processing of online transactions:

- T_p – date of charge/debit to the customer's account against the purchase of goods/services.
- T_s – date of intimation by merchant to the intermediary about the shipment of goods.
- T_d – date of confirmation by the merchant to the intermediary about delivery of goods to the customer.
- T_r – time limit of expiry of refund period as fixed by the merchant.

Now. Let's quickly understand the basic difference between the Payment Aggregators & Payment Gateways with the help of a tabular representation.

On the basis of the RBI guidelines, the PA & PG have been clearly distinguished as below:-

Factors	Payment Gateway (PG)	Payment Aggregator (PA)
Function	Intermediary between merchant and his bank	Interface/ platform of different payment gateways.
Payment mode	Only Online via Website/ Mobile App	Both Online and/or offline
Payment Options	Single	Multiple
Integration Solution	Yes	Yes
Payment Success Rate (PSR)	Depends upon how much load a payment gateway can hold.	A higher payment success rate due to integrated system.
Ownership	By public/private banks, merchants, vendors, and payment aggregators	Owned by large Fin-tech entities
Authorization	Authorized by RBI under Payment & Settlement Systems Act (PSSA) 2007.	This requires the mandatory Payment Card Industry Data Security Standard (PCI-DSS) certification.

Difference between Payment Aggregator & Payment Gateway

Throughout this manual, we will be elaborating these main points of distinction between PA & PG, which are purely based on the recent RBI guidelines.

5

Guidelines for
Authorization of Payment Aggregators

The RBI guidelines on Authorization of the Payment Aggregators is different for the Banking PAs and Non-banking PAs:

- All the non-bank PAs shall require to be authorized by the RBI in line with the Payment & Settlement Systems Act 2007 (PSSA).
- The Banks on the other hand, generally provide the services of a PA as a part of their normal course of banking operations, which is called online banking or net-banking. Hence, the Bank PAs do not require any separate authorization from the RBI.
- PA must be a company incorporated in India under the Companies Act, 1956/2013. In the MoA of the applicant company, the proposed business activity has to be mentioned as a PA.
- All the Non-banking PA that seek authorization from the RBI under the PSS Act 2007, shall submit the Form A to the Department of Payment and Settlement Systems (DPSS), RBI.

- The banks and all other PAs regulated by any financial sector regulator don't require any RBI authorization. However, this type of entities shall separately apply along with a NOC from their regulator, within 45 days of obtaining such a clearance.

BANKING PA   NON-BANK PA

- The deadline for non-banking PA to apply for RBI authorization is 30th June 2021.
- They can however, continue their operations till they receive any further intimation from the RBI regarding the processing of their application. Importantly, their business activity of PA services shall be separated from that of e-commerce business.

The RBI has clearly defined the capital requirement for becoming eligible to offer Payment Aggregator service. The guidelines for the same are given below:

- Net-worth
- Composition of Net-worth
- FDI
- Net-worth Certificate

1. *Net-worth for RBI authorization:*

Threshold limit for the net worth of PAs shall be-
- ₹15 crore by 31st March 2021 and
- ₹25 crore by 31st March 2023.

This net-worth shall be maintained thereafter forever.

Thus, new PAs at the time of application for RBI authorization must have a minimum net-worth of ₹15 crore. By the end of 3rd financial year of grant of RBI authorization, they must attain a net-worth of ₹25 crore.

The above criteria can be understood with the help of the table given below:

Non-bank PA	Date of RBI Authorization	Date when Net-worth=₹ 15 Cr.	Date when Net-worth=₹ 25 Cr.
Established PA	Before or on 30/06/2021	Date of application or 31/03/2021, whichever earlier	31/03/2023
New PA	20/03/2020 01/04/2020 01/03/2021 01/04/2021	On date of application	31/03/2022 31/03/2023 31/03/2023 31/03/2024

2. *Composition of the net worth of PAs:*

The net-worth of the all the PAs shall consist of the following:
- Paid-up equity share capital;
- Preference shares that are convertible to equity*;
- Free reserves,
- The balance must be in share premium account and capital reserves representing surplus due to sale of fixed assets.

Notes:
- The above-mentioned compulsorily convertible preference shares can be non-cumulative/cumulative. These must be convertible into equity.
- All the shareholder agreements in this regard should restrict any withdrawal of such preference share capital at any point of time.

However, this must not include the following:

- Reserves created by the revaluation of fixed assets adjusted for accumulated loss balance;
- Book value of intangible assets;
- Deferred revenue expenditure (advertisement, promotion etc.), if any

3. *Foreign Direct Investment (FDI):*

All the non-bank entities having FDI shall be governed by the Consolidated Foreign Direct Investment policy as well as the relevant FEMA regulations in this regard.

Our FEMA Advisory team can provide you expert help and guidance regarding the same.

4. *Net-worth Certificate:*

Sample of a Net-worth Certificate

The newly incorporated non-bank PA entities generally do not possess audited financial statements. Hence, for RBI authorization, these non-bank PA applicants shall submit a certificate of evidence from a practicing CA in the enclosed format, substantiating the current net-worth. however, this must be accompanied with a provisional balance sheet.

5. *Non-compliance:*

In case a PA fails to comply with the net-worth requirement within the specified time frame, he shall immediately discontinue his payment aggregation business. Any banks holding nodal / escrow accounts for such PA entities must regular monitor and report the compliance status in this regard to the RBI.

The RBI has stipulated clear-cut norms for the good governance and professional conduct of the PA entities. In this regard:

- The directors of the applicant PA are required to submit a declaration in the enclosed format that the promoters of the entity satisfy the 'fit & proper' criteria as prescribed by the RBI.
- The RBI is authorized to monitor the 'fit & proper' status of the applicant PA bank entity with the proper assistance of some regulators and government departments. Applications of ineligible entities shall be rejected.
- All the Agreements between PAs, merchants, acquiring banks, and other stakeholders must clearly define the responsibilities all the involved parties in-
  - *Handling complaints,*
  - *Refund/failed transactions,*
  - *Refund policy,*
  - *Customer grievance redressal (with turnaround time)*
  - *Dispute resolution mechanism, Reconciliation*

- For handling the complaints, dispute resolution mechanism, and for the processing of refunds, etc., the PAs must have a policy that is approved by the Board (of RBI). The policy in this regard must be as such that the RBI guidelines on Turn Around Time (TAT) for resolution of complaints of failed transactions are duly met.

REFUND POLICY
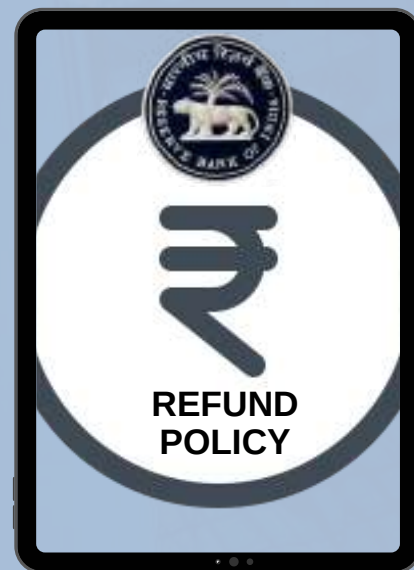
- For this purpose, PA applicant has to appoint a Nodal Officer who shall be responsible for Customer grievance handling. The details of such nodal officer have to be displayed on the business portal of the PA applicant.

NODAL OFFICER

- Following information has to be comprehensively displayed on the business portal/mobile app of the PA applicant:
  - *Merchant policy,*
  - *Customer review/grievances,*
  - *Privacy policy and*
  - *Other T&C*

8

Provisions for
Anti-Money Laundering

Just like all other types of financial institutions, the Payment Aggregators The guidelines issued by the Department of Regulation, RBI, as regards KYC, Anti-Money Laundering (AML) and Combating Financing of Terrorism (Terror funding) shall apply to all the PA entities.

As a matter of fact, the recommendations of FATF on Anti Money Laundering (AML) and Combating Financing of Terrorism (terror-funding) standards have now become global benchmark for framing AML and anti terror-funding policies by the regulatory authorities.

Provisions of Prevention of Money Laundering Act, 2002 and Rules framed thereunder, as amended from time to time, shall also be applicable to all the non-bank PA entities.

9 Policy for Merchant On-boarding

Undoubtedly, a seamless payment aggregator is sought after by its users for its swiftness, aptness and user-friendly features.

- Accordingly, the PAs shall put in place a policy for seamlessly on-boarding the merchants on its portal/mobile app. This policy must be approved by the Board (RBI).
- To ensure effectiveness of its merchant on-boarding policy, the PAs shall conduct background checks of the member merchants. Such surprise checks are intended to ensure that the merchants do not have any wrong intent to dupe their customers, or to offer fake / counterfeit / prohibited services or transactions.
- Moreover, the member merchants should clearly specify his terms and conditions of the service and TAT to process returns & refunds on his business portal.

- As discussed above, all the PA entities require the mandatory Payment Card Industry Data Security Standard (PCI-DSS) certification.
- Additionally, the PA entities are supposed to verify the PCI-DSS Standard as well as the Payment Application-Data Security Standard (PA-DSS) compliance on the part of the merchants while on-boarding them on their portal.
- There should be security audit of the on-boarded merchant to check compliance of privacy policy. Merchant portal must not save any private detail of the customer.

Customer Privacy

PCI-DSS

Customer
Data Security

PA-DSS
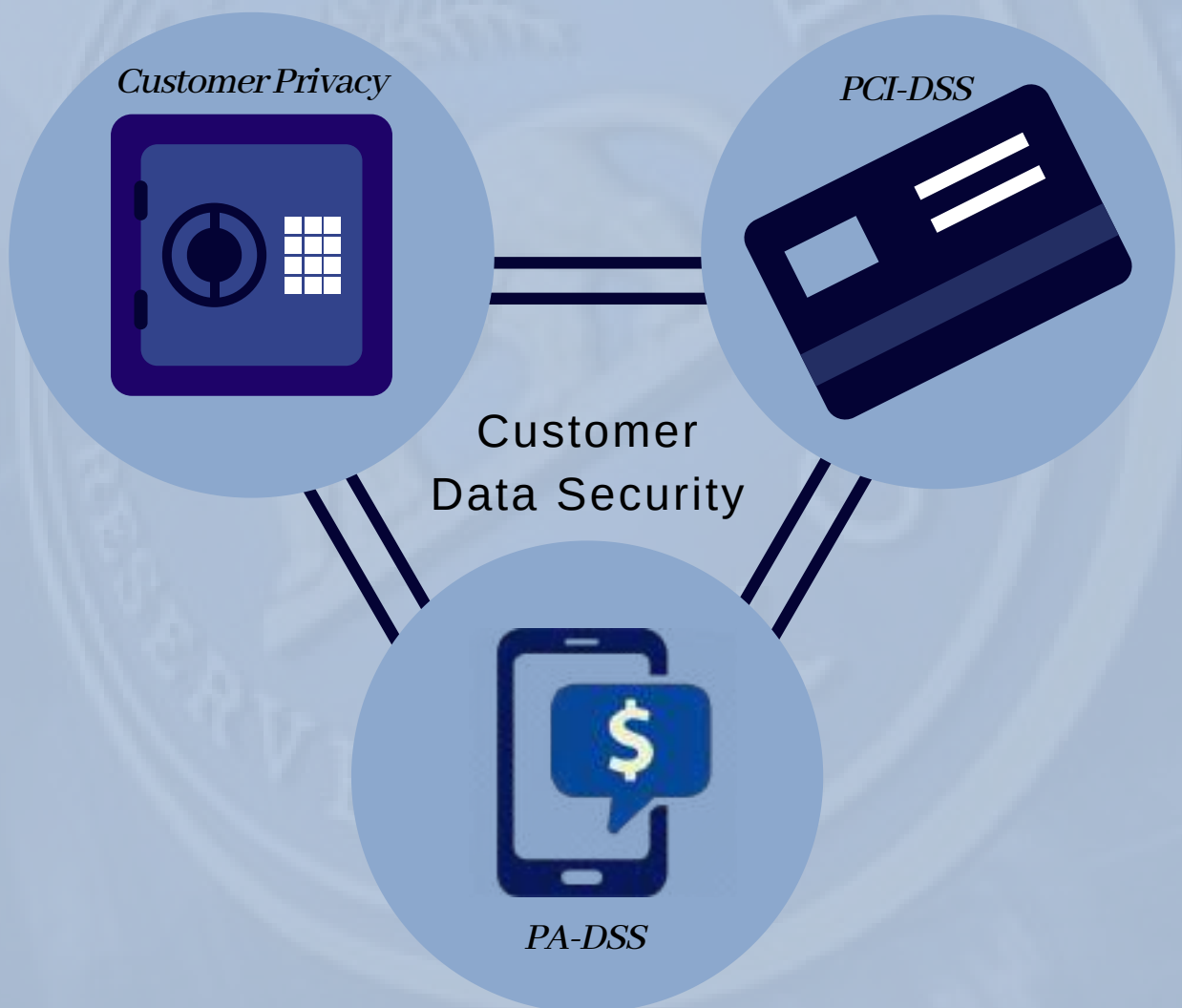
10

Escrow Account

and its Management

As per the RBI guidelines, all the Non-bank PAs are required to deposit the amount collected from merchants in an "escrow account".

This is an account which shall be opened with any of the RBI scheduled commercial banks. Hence, the activity of the PAs shall be deemed as 'designated payment systems' u/s 23A of the Payment and Settlement Systems (Amendment) Act for the maintenance of this escrow account.

What is an Escrow Account?

In simple words, an escrow account is a 3rd party account (opened with a scheduled bank), where the money is temporarily deposited before it is finally transacted to the destined party account.

Usually, the escrow accounts are opened in case of huge transaction such as those related to real estate projects. These days, many e-commerce sites also prefer escrow accounts as an alternative mode of transactions. The most common example is of the e-wallet system in some B2C sites.

Here, we shall be discussing in detail about the RBI guidelines for the Escrow bank accounts, which the merchants open with the scheduled commercial banks for size-able transactions.

I. Guidelines for managing Escrow account

- The PAs shall maintain Escrow account with only one scheduled commercial bank at a time.
- In case of a need to shift the escrow account some other bank, the same shall be done timely without hampering the payment cycle of the merchants. Ideally, this process must be done with proper advice from RBI.

II. Deposit into Escrow account

- Deduction of any Amount from a customer's account shall be credited to the escrow bank account on Tp+0 / Tp+1* basis.
- The same rules apply to the non-bank PA entities, where e-wallets are used for payments.

Please refer to the key to the timelines given above.

III. <u>Final settlement with the merchant</u>

Here are the rules for Final settlement with the merchant by the PA:

- If PA is responsible for delivery of goods/services (such as Amazon/Flipkart), the payment to the merchant shall be not later than on $T_s + 1$.
- If merchant is responsible for delivery (any product-selling site), the payment to the merchant shall be not later than on $T_d + 1$.
- In case there is agreement with the merchant for keeping the amount with the PA till the refund period expires, the payment to the merchant shall be not later than on $T_r + 1$.
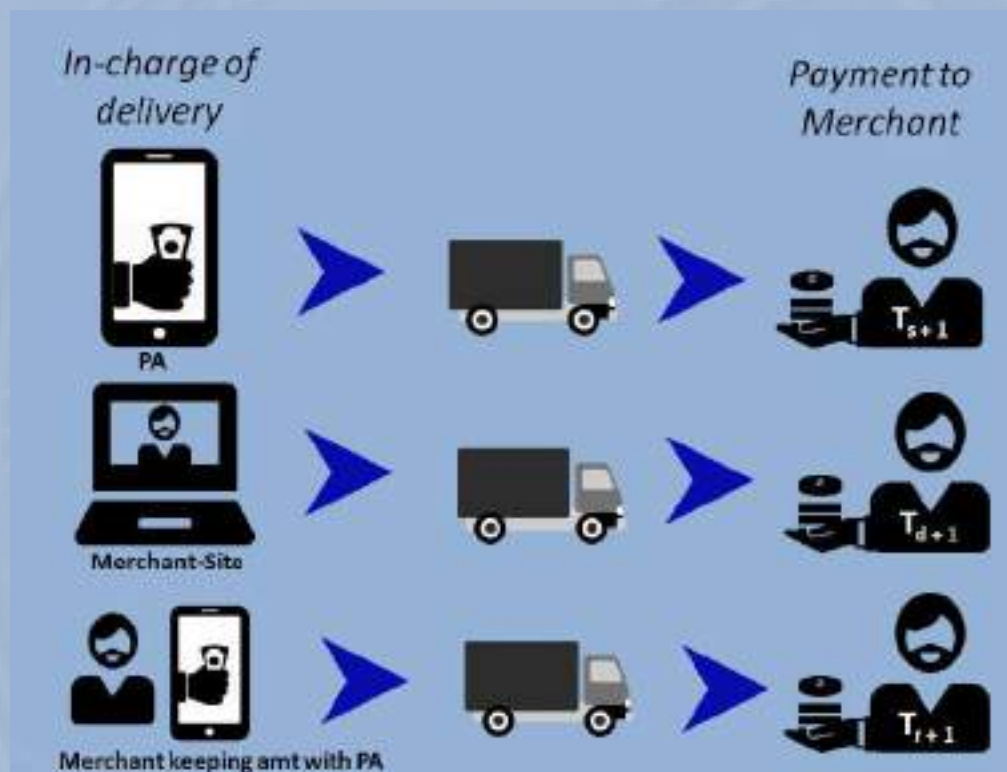
IV. <u>Refund procedure:</u>

The RBI guideline states that in case any transaction is reversed, and where the PA has received funds, it should be done through the PA channel only. However, there's an exception that if as per the contract, the refund is directly managed by the merchant in the knowledge of the customer, refund may be done directly.

Escrow Account

Permitted Debits & Credits

There are clear guidelines as to when to open escrow accounts. The rules for permitted credit and debit to the Escrow account are given below:

Allowed Credit towards-

- Payment from customers towards purchase of goods / services.
- Pre-payment by merchants / PAs.
- Refunds for failed, disputed, reversed or cancelled transactions.
- Payment received to forward transfer to the merchants in case of promotional activities, such as cash-backs, discounts etc.

Allowed Debit towards-

- Payment to the merchants.
- Payment to any other account subject to specific directions from the merchant.
- Refunds for failed, disputed, reversed or cancelled transactions.
- Commission to the intermediary.

Grievance Redressal
& Dispute Management

There must be in place a formal and openly disclosed customer grievance redressal & dispute management mechanism:

How should a complaints management system be?

- PA shall appoint a nodal officer to handle the customer complaints / grievances and the escalation matrix.
- Dispute resolution mechanism shall be binding on all the participants of the transactions.
- The Dispute resolution mechanism shall contain the following:

  - 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 of these stages

Risk Management
& Fraud Prevention

Robust risk management system is essential to mitigate chances of fraud and to ensure customer protection.

Salient features of Risk Management:

- Adequate information and data security infrastructure and systems must be there.
- RBI approved information security policy for the safety and security of the payment systems.
- There must be mechanism for monitoring, handling and follow-up of cyber security incidents and data breach.
- Data breach must be reported immediately to the DPSS, RBI.
- PAs shall not save the customer private credentials within their database or the merchant server.
- PAs shall submit the System Audit Report, incl. cyber security audit conducted by CERT-In impaneled auditors, within 2 months of the close of their financial year to the respective Regional Office of DPSS, RBI.
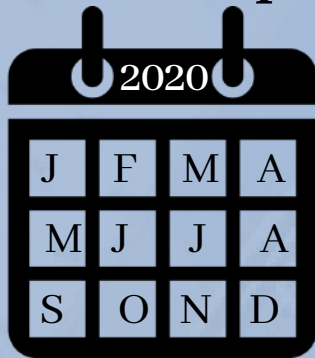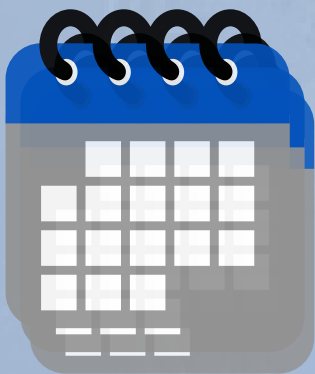
14 Important Reports

Here are the mandatory reports to be submitted by the non-bank PAs that are authorized by the RBI:

I. *Annual Reports:*

- Net-worth Certificate: To be submitted by 30th September every year.
- IS Audit Report and Cyber Security (external) Audit Report: 31st May every year.

II. *Quarterly Reports:*

- Auditors' Certificate of Maintenance of Escrow Account Balance – by 15th of the next month of the quarter ending.
- Bankers' Certificate of Escrow Account Debits & Credits – by 15th of the next month of the quarter ending. (Internal Audit).

III. *Monthly Report:*

- Report of Statistics of Transactions Handled – by **7**th of every next month

IV. *Non-periodic Reports:*

- Declaration & Undertaking by the Director: Whenever Change in director(s)
- Cyber Security Incident Reports: by **7**th of next month of whenever incident occurs.

Technology Guidelines
For PAs & PGs

RBI has set out comprehensive guidelines for IT & Data security, which are binding only on the PAs but are equally recommended to the PGs. Here are those important guidelines:

I. *Data security guidelines:*

- The entities should conduct comprehensive risk assessment of their staff, esp. IT, and the business process environment, etc., to check risk exposures, with remedial measures and residual risks.
- Reports on risk assessment, data security compliance status, and audit reports must be submitted to the Board.
- Data security standards like PCI-DSS, PA-DSS are mandatory for PA entities. However, the Payment gateways are required to be RBI authorized as per the PSSA 2007.
- The entities should maintain an "enterprise data dictionary". This shall include the basic data syntax rules for an organisation. This will facilitate seamless data sharing across applications and systems, besides preventing development of inappropriate data elements.
- Application Access: Access to the application must be very gradual and must commensurate with increasing of the job responsibilities.
- Regular assessment of the requirement for trained personnel with required IT skills.

II. *Other Important Aspects:*

- Vendor Risk Management
- Cryptographic Requirement
- Forensic Requirement
- Data Sovereignty
- Data Security in Outsourcing.

III. *Important advices for data security within the PA business environment:*

- The customer card credentials and other privy data shall never be stored within the database or the server that is accessed by the merchant.
- The ATM PIN of customer shall never be offered or preferred as a way of authentication for card-not-present transactions.
- Instructions for storage of payment system data shall apply as applicable to PSOs.
- The refund procedure shall be done with the original channel of transaction only, except when an alternate mode is specifically opted by the customer himself.

Thank you!

For more info, please contact:-

Mr. Narendra Kumar

Managing Partner