

AN ASSESSMENT OF THE LIABILITY OF PAYMENT AGGREGATORS IN INDIA
UNDER THE RBI GUIDELINES.

Vyshnavi Praveen & Ananya Soni***

Abstract: *The digital banking sector is one of the fastest developing sectors with millions of users worldwide. The pandemic and demonetisation have been some of the crucial accelerating factors in aiding this boost. Payment aggregators are one such digital asset that has been invaluable in connecting merchants and customers by bridging the technological gap. With digital banking growing so much in terms of popularity in such a short span, it is no doubt that there have been increased instances of fraud, scams and theft which has raised some security related questions. In an age when more individuals are opting for digital payment methods, there is a dire need to ensure that there is a safe and sound financial, technological infrastructure network present in the country and this resulted in the RBI coming up with the first ever concrete guidelines for payment aggregators: The Guidelines on the regulation of Payment Aggregators and Payment Gateways in March, 2020. These guidelines bring about a new era in Payment aggregation business by providing for mandatory licensing, dispute resolution mechanisms and verification. Although these guidelines have been a commendable step towards the advancement of the online payment and banking sector- how do these guidelines perform in terms of comprehensiveness and adequacy while imposing liability?*

Keywords: *Payment Aggregator, Payment Gateway, RBI, Digital Banking, Liability*

* IV Year, B.A. LL.B. (Hons), Tamil Nadu National Law University, Tiruchirappalli.

** IV Year, B.Com. LL.B. (Hons), Tamil Nadu National Law University, Tiruchirappalli.

I. HISTORY OF PAYMENT AGGREGATORS IN THE INDIAN BANKING SCENARIO

In order to completely understand and analyse the current position of payment aggregators, it is vital to take a look at the history of payment aggregators and the evolution of the payment aggregator history in India. By tracing the history of these intermediaries one will be able to understand the improvements to the area and analyse the various shortcomings with regards to the existing legislations.

Payment methods in India have most certainly evolved to a great extent since its inception. Online banking has perhaps been one of the biggest successes of Indian history and has become more widely accepted with each passing day. In 1980, the Central bank of India released the first ever credit card in India, which was followed by MasterCard in 1988 and many other such banks by 1990.

Online Banking was first introduced in India by the Industrial Credit and Investment Corporation of India ('**ICICI**') Bank in 1996, and other banks quickly followed suit. This marked the beginning of the digital banking era in India.¹ Following this, in 2008 the National Payment Cooperation of India ('**NPCI**') was launched by the Reserve Bank of India ('**RBI**') to help develop and expand the online payment infrastructure in India. The NPCI did just that by bringing about innovations in retail payment systems. Some retail payments products brought about by NPCI include Immediate Payment Service ('**IMPS**'), RuPay card scheme, Unified Payments Interface ('**UPI**'), National Automated Clearing House ('**NACH**'), Aadhaar-enabled Payments System ('**AePS**'), and Bharat Bill Payment System ('**BBPS**').

The NPCI did much with regards to improving the state of digital India and some of the major contributions made include:

1. Banking cards: Under the NPCI much was improved in terms of the quality of cards and the services they offered. Prepaid cards were brought about and new safety features such as Personal Identification Number ('**PIN**') and One Time Password ('**OTP**') were introduced. Apart from this, NPCI made the process of online payments easier.

¹*Digital payments and their impact on the Indian economy*, INDIA BRAND EQUITY FOUNDATION, (Sept 10, 2022) <https://www.ibef.org/research/case-study/digital-payments-and-their-impact-on-the-indian-economy#:~:text=In%201996%2C%20Industrial%20Credit%20and,Citi%20launched%20online%20banking%20facilities.>

2. Unstructured Supplementary Service Data ('USSD') channel: This was an innovative feature that enabled banking services to take place using a mobile interface even without the use of internet which revolutionised the payment game in India.

II. UNDERSTANDING THE NATURE OF PAYMENT AGGREGATORS

Payment Aggregators ('PA') thought not a completely new concept to the Indian markets, are relatively a little more complex to understand. Before going into the various intricacies of the concerns associated with PAs, the liability and the future scope, one needs to understand the true nature of the concept of payment aggregation.

A. WHO ARE PAYMENT AGGREGATORS AND WHAT DO THEY DO?

According to the Guidelines on Regulation of Payment Aggregators and Payment Gateways put out by the RBI in March, 2020, Payment Aggregators are defined as 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.²

Essentially, PAs act as intermediaries by providing the required technological infrastructure and help bridge the gap between the online merchant, buyer and the payment instruments to facilitate the transfer of funds without actually handling the funds themselves. By being the bridge between consumers at one end, and merchants at the other end, these service providers play a role in processing and completion of the payment transactions. They could be engaged by a bank, a merchant, or a biller. As to the various services offered by PAs, they broadly include:

- Providing the necessary interface for the fund transfer/payment.
- Entering into agreements with the billers.
- Managing the various operational complexities that arise out of using various different payment instruments.
- Providing all the banks with a standard method of dealing with the bill data.
- Managing the various utility requirements, consolidated pay-outs and other various service delivery aspects.

² Reserve Bank of India, Guidelines on Regulation of Payment Aggregators and Payment Gateways, DPSS.CO.PD. No.1810/02.14.008/2019-20, (Issued on Mar 31, 2021).

Payment aggregators work by interacting with various entities to ensure that transactions are securely carried out between merchants and customers. The major steps involved are:

1. The PG runs a fraud check and encrypts the card details of the customers.
2. The acquiring bank collects relevant details.
3. The card network runs a fraud check.
4. Transactions are approved by the issuing banks.
5. The card company communicates either its approval or denial of the transaction.
6. This approval or denial is communicated to the customer via the PG.
7. Upon the approval, the acquirer requests money from the issuer

In the present technology driven era, it is safe to say that payment aggregators have become indispensable given the heavy reliance by online retailers, which calls for an increased need to monitor and regulate these entities.

B. PAYMENT AGGREGATORS V. PAYMENT GATEWAYS

Payment aggregators and Payment Gateways ('PG') are often used interchangeably however they are not the same. PGs are essentially a software service that enable companies or merchants to process online payment transactions on their interface. They allow acceptance of payment in various forms such as UPI, debit card, or a credit card. A PA on the other hand, is a service provider that aggregates and provides various payment acceptance services to merchants. The major difference is the fact that while a gateway is for e-commerce websites/apps, an aggregator digitises online and/or offline payment touchpoints³.

While PAs are largely owned by fintech players such as RazorPay and RuPay, PGs are owned by public and private banks, vendors and even other PAs. PGs typically deal with data on the front-end whereas PAs are capable of going through the underwriting process of the concerned banks.

PGs in India permit payments on the website/app only using a few select options but there is a wider choice offered by PAs including UPI, cards etc. The bottom line is that while PAs are the payment interface, PGs are simply the payment intermediaries.

³ Chaitali Bhatia, *what differentiates a Payment Aggregator from a Payment Gateway?* EZETAP BY RAZORPA, (Sept 10, 2022), https://corp.ezetap.com/blogs/what-differentiates-a-payment-aggregator-br-from-a-payment-gateway_

C. PAYMENT AGGREGATORS IN THE CONTEXT OF BANKS: HOW DO THEY DIFFER?

Now that it has been established that PAs are merely the interface that helps merchants collect funds, it brings us to the next question: how do these aggregators differ from traditional banks in terms of functions and duties?

Traditionally speaking, in order to be classified as a bank, an organization/ institution has to perform certain core functions including: Take deposit amounts, take current accounts, issue and pay cheques and collect cheques both crossed and uncrossed from their customers. This was elaborated in Sir John Paget's definition of banking. Furthermore, under the Banking Regulations Act, 1949 "banking" means the accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise, and withdrawal by cheque, draft, order or otherwise⁴ and additionally a banking company is one that provides banking services.⁵ From the definition of payment aggregators, it is clear that they perform features including acceptance of funds on behalf of merchants which is a crucial element of banks however this is applicable in the most limited sense. In the context of banks, PAs are more on the lines of an intermediary that supports transfer of funds between one bank account (customer) to another bank account (vendor).

Looking at the definitions relating to who is a banker and what are banking services in the Indian context, it appears that PAs do not fit the definition of a banker by providing banking facilities for a few reasons:

1. There is an absence of the cheque deposit and issuance feature
2. The deposited funds are not payable upon demand and have to follow certain channels
3. They are not open to the general public and only apply to a merchant and customer scenario.

In order for an entity to be held as a bank/ banker, these banking services need to be the primary business of the organization and these banking functions (including accepting deposits from general public and offering loans) need to be done for the main aim of profit making⁶. Payment aggregators typically charge merchants based on each transaction that is carried out and this amount may be fixed or varied. The differentiating factor here is the fact that the primary

⁴ Banking Regulation Act, § 5(b), No. 10, Acts of Parliament, 1949 (India).

⁵ *Id.*, § 5(c).

⁶ *Id.*, § 7.

service is not that of banking but rather providing the financial technology to enable payments. Just because the PAs accept funds on behalf of the merchants does not mean that they may be called banks.⁷ Interestingly enough, more and more banks owing to the popularity of such payment systems have introduced their own PAs.

III. THE GUIDELINES ON REGULATION OF PAYMENT AGGREGATORS AND PAYMENT GATEWAYS

As discussed previously, PAs and PGs essentially form the backbone of the modern banking sector in the retail space and the increased number of upcoming PAs has pushed the RBI to release guidelines relating to the functioning of such intermediaries. The increased traffic in this area caught the eyes of regulatory bodies such as the RBI which stepped in and decided to introduce certain measure to ensure increased scrutiny and to regulate the actions of the many aggregators that came about. This resulted in the RBI, with its powers from the Payments and Settlement Systems Act,⁸ introducing the Guidelines on Regulation of Payment Aggregators and Payment Gateways in March 2020.⁹ The guidelines were brought about in a bid to ensure that more such aggregators come within the purview of the RBI and to increase scrutiny to prevent rising instances of data breach and fraudulent activities. While there are banking and non-banking PAs, these guidelines only apply to the non-banking entities.

A. WHY THE NEW GUIDELINES?

As new as the concept sounds, PAs have actually been around for a while and are not a new concept. For example, BillDesk was one of the first and most comprehensive PAs to have been introduced all the way back in 2003.¹⁰ Despite PAs having existed for so long, there was little to no regulation regarding their activities which emerged as a cause for concern. PAs and PGs were mostly unregulated until the RBI released directions for opening and operation of accounts and settlement of electronic payment transactions involving intermediaries in November 2009.¹¹ Under these guidelines, PAs were treated as intermediaries who were

⁷ *Ramalingam Pillai v. Sankara Iyer and Ors* [1964] 1964 Mad 424.

⁸ The Payment and Settlement Systems Act, § 3, No 51, Acts of Parliament 2007 (India).

⁹ *Supra* note 2.

¹⁰ *Shaping the ways payments are made and accepted*, BILLDESK, (Sept 12, 2022), https://www.billdesk.com/web/about_us#:~:text=Over%20the%20next%20decade%20and,stage%2C%20governments%20and%20financial%20institutions.

¹¹ Reserve Bank of India, Directions for opening and operation of Accounts and settlement of payments for electronic payment transactions involving intermediaries, RBI/2009-10/231 DPSS.CO. PD. No.1102 /02.14.08/2009-10. (Issued on Nov 24, 2009).

required to maintain a nodal bank account and comply with the Information Technology Act of 2008¹². However, these guidelines didn't provide a comprehensive framework for the operation of Pas, and had no mandatory licensing requirements which resulted in the PAs continuing to remain vastly unregulated.

The use of these new and unregulated PAs did not help the general consumer population as indicated by a Global Tech Support Scam Research report put out by Microsoft in July 2021, suggesting that 31% of Indians using online payment and indulging in online retails had lost money to scams, which was a 238% increase as compared to 2018¹³. This clearly shows a positive correlation between and higher instances of frauds and scams, as a result of increased reliance on PAs

Perplexed by this growth, the RBI decided to introduce the guidelines relating to PAs and PGs in 2020. The new guidelines calling for mandatory licensing of non-bank PAs came as a solid move in the direction towards the regulation of these PAs. In 2022, RazorPay, Pinelabs and Stripe were amongst some of the first few entities to have received this license from the RBI.¹⁴

B. NEW GUIDELINES, NEW STAKES: INCREASED LIABILITY?

It is no doubt that a lot will change with the new guidelines in place. Firstly, the new guidelines specifically state that PAs shall have a minimum net-worth of ₹15 crore at the time of application for authorisation and shall attain a net-worth of ₹25 crore by the end of third financial year of grant of authorization and this ought to be verified by a Chartered Accountant ('CA'). Under these guidelines, all PAs who are unable to comply with the capital requirement within the prescribed period will mandatorily be required to close up their aggregation business. It is interesting to see that in this case, the liability has been placed on the nodal accounts/escrow accounts to monitor and report compliance with this regard.¹⁵

In the case where a non-bank entity carries out an aggregation business that they will be required to maintain an account with a bank (escrow/nodal) indicates a banker customer relationship between the PA and the bank. The liability of ensuring compliance in terms of the

¹² The Information Technology Act, No 13, Acts of Parliament, 2008 (India).

¹³ *Global Tech Support Scam Research Report*, MICROSOFT, (Jul 2021), <https://news.microsoft.com/wp-content/uploads/prod/sites/45/2021/07/Microsoft-India-Tech-Support-Fraud-Survey-2021.pdf>.

¹⁴ Subrata Panda, *RBI clears payment aggregator licence for Razorpay, PineLabs & Stripe*, BUSINESS STANDARD, (Sept 14, 2022) https://www.business-standard.com/article/finance/rbi-clears-payment-aggregator-licence-for-razorpay-pinelabs-stripe-122070800873_1.html

¹⁵ *Supra* note 4.

capital stipulation as per the guidelines appears to fall almost entirely upon the banks with no apparent regulatory or supervisory body in place. Additionally, the guidelines make no mention of what is to happen in the event that banks themselves fail to comply with these provisions. It is rather strange that from the guidelines, no liability seems to be imposed on the PAs in this case. There are several issues with leaving this compliance aspect upon banks: Firstly, owing to the customer and banker relationship between these PAs and banks, there appears to be no actual motive or benefit from banks and hence there is no benefit that actually comes of banks wanting to alter the terms of their relationship with these PAs which would also mean loss of business to the bank. Additionally, there is no guarantee that banks will be held liable in the case of any irregularity to this regard. The lack of accountability and a proper reporting channel along with a lack of clarity as to the authority vested to banks remains uncertain. The mention of “monitor and report” compliance here remains largely ambiguous with regard to the level of scrutiny that banks have to undertake, the rights and powers granted to them in this regard and also the proper channel of reporting that ought to be followed.

The guidelines mention that the Know Your Customer (‘**KYC**’) Directions¹⁶ as updated from time to time will apply to PAs.¹⁷ As per the directions of the KYC circulars, all regulated entities are required to undertake KYC measures for the customers as soon as there is the creation of an account-based relationship. It remains rather unclear from the guidelines as to whether PAs providing services to various merchants will have to undertake these KYC measures with every merchant even if there might not be an account-based relationship. Another point to note is that while opening accounts with their respective banks, merchants, and customers would have already gone through the KYC process. With these requirements already in place, it seems rather frivolous to require PAs to additionally carry out this KYC process with merchants. Furthermore, considering these guidelines apply to non-banking PAs and seeing how the funds are maintained in an escrow account, there is no direct relationship between the account and the merchant, thus it comes off an unnecessary step. There are however arguments that favour this KYC requirement as it might serve as an additional layer of security and verification, which might curb online merchant fraud.

With regards to the entire governance system, a major concern of even the users of such PA systems has been with regards to the lack of transparency. The guidelines state that agreements

¹⁶ Reserve Bank of India, Master Direction - Know Your Customer (KYC) Directions, RBI/DBR/2015-16/18 (updated on May 10, 2021).

¹⁷ *Id.*

should be entered between PAs, merchants, acquiring banks with regards to handling refund/failed transactions, return policies and customer redressal.¹⁸ This clause fails to uniformly affix liability upon one particular party. In the case of banks themselves, a clear picture painting the liability of both customers and the bank has been painted by the RBI Circular on Customer protection,¹⁹ and backed by various cases over the years.²⁰ In most of these cases, liability is established based on contributory actions, depending on the degree of involvement of the customers in transactions.

Additionally, this circular seems to discount the fact that more parties are involved in such online payment methodologies using PAs as opposed to direct use of banking features. It becomes extremely complicated to identify the parties considering the chain that ensues post approval of payment. In such a circumstance, by requiring the involved parties to decide amongst themselves the level of liability that each entity assumes only results in increased hesitation and as a result, more inconvenience for the users of such facilities. This method further allows for more deadlock situations where parties are unwilling to negotiate and come to consensus. Further, this also leads to lack of uniformity relating to liability amongst various PAs, undermining the very purpose of these guidelines. In 2016, the RBI issued a master circular relating to the reporting of fraud by commercial banks and a few select financial institutions, which doesn't include PAs. Resultantly, there is a lack of a properly laid down framework for the reporting of fraudulent instances by PAs and other intermediaries.²¹

Further, with regard to the process of merchant onboarding, the circular dictates that PAs are required to carry out background and antecedent checks to verify the authenticity of the merchant.²² The guidelines specifically require all PAs to verify the authenticity of the merchants, however makes no mention of the extent of this power or its limitations. Furthermore, these PAs are required to carry out security audits to ensure that merchants do not save the details of customers however there is no clarification provided by the RBI or any other regulatory body as to the mode of conducting such audit and the specifics of the same, which might lead to breach of data.

¹⁸ *Id.*

¹⁹ Reserve Bank of India, Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI/2017-18/15, (issued on Jul 6, 2017).

²⁰ *Punjab National Bank and Anr. v. Leader Valve* (2020) CPJ 92 (NC).

²¹ Reserve Bank of India, Classification and Reporting by commercial banks and select FIs, RBI/DBS/2016-17/2, (Updated on Jul 3, 2017)

²² *Id.*

Further, the guidelines do not mention whether this requirement extends to PAs in instances when the PA provides its services to an e-commerce entity (who onboards sub-merchants), and whether they will be required to undertake KYC for the sub merchants as well, since the delivery of goods and services is by the sub-merchants. The guidelines also fail to address what ought to be done in the event where a merchant employs the services of a PA solely for collection of amounts from customers where the actual transactions are conducted offline. In addition to this, PAs will be required to ensure whether or not the terms and conditions have been listed on the website of the merchant. Additionally, merchants may have availed listing services from third parties and might not be in a position to carry out these listing requirements. The RBI has issued no clarification as to the powers and authority of PAs in carrying out this compliance.

The guidelines (clause 7.3) also require the PAs to check Payment Card Industry-Data Security Standard ('**PCI-DSS**')²³ and Payment Application-Data Security Standard ('**PA-DSS**')²⁴ compliance of the infrastructure of the merchants on-boarded. However, the guidelines also dictates that merchant sites are not to save date related to customer card , and that the PA may carry out security audit of the merchant to check compliance, as and when required²⁵. It is an interesting requirement considering how merchants are not permitted to store card related data. Additionally, PA-DSS and PCI-DSS may prove to be rather onerous on new, small and medium business entities which is another concern regarding these guidelines.

The guidelines also call for a strong risk management system to be put in place with PAs with the help of the Baseline Technology Related recommendations. However, these are mere recommendations and have no binding value. Adding on, there exists no regulatory body ensure that PAs comply with these regulations.

IV. A LIABILITY ASSESSMENT

Now that we have understood the key areas of change relating to the new guidelines along with the concerns associated with them, we need to move on to the next issue: What is the actual extent of liability of PAs and who regulated this liability?

²³ PCI, *Payment Card Industry Data Security Standard*, (Sept 14, 2022) <https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4-0-SAQ-D-Merchant.pdf>

²⁴ PCI, *Payment Application-Data Security Standard*, (Sept 14, 2022) https://listings.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf.

²⁵ *Id.*

There are several concerns that may be associated with an online PA business including data privacy and security of the customers, acquiring bank and unauthorized transactions etc. Data privacy has perhaps been one of the most pressing issues especially in recent times. The primary concern remains that given the existence of multiple parties, who should be held liable for breach? The answer depends upon who handles the data, the nature of the data, and as to who processes or collects this data. As per the guidelines released by the RBI, PAs and the merchants would not be allowed to store any data. Considering the PA works by providing the technological infrastructure, it is natural that there are degrees of liability towards the various parties involved.

A. LIABILITY TOWARDS CUSTOMERS

As already evidenced by the way PAs work, they are a vital player in facilitating online transactions between merchants and customers. That being said, there is an implied and express liability that the PA has towards the customers

Firstly, banks are liable as per the new guidelines to ensure that there is a comprehensive grievance redressal and dispute management framework including the appointment of a nodal officer to handle customer grievances and so on. It is evident that the liability in the event of customer grievances relating to the disputes lies almost entirely upon the PA. It is also the liability to ensure that all details pertaining to this dispute redressal mechanism is properly published on the merchant's website. It appears that the burden of ensuring the success of payments and transactions is on the PAs and rightly so considering the fact that it is due to this technological infrastructure that transactions are carried out. However, while looking at the entire issue from the customers' point of view, it appears that in most cases a customer would be more comfortable dealing with the merchant directly relating to such queries instead of the PA. This is due to the fact that while a customer enters into an agreement to purchase anything, they maintain a relationship only with the merchant. This is probably the reason why in several cases where merchants engage PAs, there is a collaborative effort to ensure that redressal services are offered to the customers in an easily accessible manner. Under the guidelines, the PAs will be liable for promptly initiating refunds and managing failed transactions in accordance with the prescribed RBI directions.²⁶ This measure ensures that customers are

²⁶ Reserve Bank of India, Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems, RBI/2019-20/67 DPSS.CO.PD No.629/02.01.014/2019-20, (issued on Sept 20, 2019).

adequately protected against any possible mismanagement on part of the PAs and also have redressal under the Reserve Bank - Integrated Ombudsman Scheme, 2021²⁷

Although it is understood from reading the guidelines that this liability is vested upon the PA, there is ambiguity regarding the actual consequences and punishments in the case of non-compliance.

Similarly, with respect to fraud prevention and risk management, PAs are required to install good and secure technology infrastructure to ensure minimization of risk and the chances of fraud. The liability here is placed on the board to approve a security and safety policy.²⁸ Under the relevant guidelines, there is an effort to create a working relationship between PAs and the DPSS, RBI, Central Office, Mumbai and CERT-In (Indian Computer Emergency Response Team). This also indicates the accountability towards regulatory and vigilance bodies on part of the PA. Additionally, PAs are not permitted to store any of the personal data of any customer and are required to comply with the same standards as applicable to Payment System Operators ('PSO')²⁹. As per this, the PAs will be mandated to store data only in systems located within India, which is something enshrined in the GDPR as well³⁰. Even in this instance, the PAs are liable to ensure compliance and report the same to the RBI. System Audit Reports (SAR) conducted by the CRET-In add an additional layer of liability on the PAs and ensure that there is mandatory compliance and increased accountability. When there is data stored there invariably also is data sharing and data processing. Brings us to the question of when will the PA be bound to disclose any shared data if any? While there is no explicit provision that outlines this, we may apply the same rationale behind banks and their data sharing. Typically, data may be shared: when there is prior consent, when there is legal compulsion or if there exists a greater public duty. Legal compulsion might perhaps be one of the most solid grounds for such PAs having to disclose information E.g., Sec 131 of the Income Tax Act, 1961³¹. The Indian courts too have on multiple occasions upheld the banks duty to disclose information where there is a legal compulsion.³²

²⁷ Reserve Bank of India, The Reserve Bank - Integrated Ombudsman Scheme, 2021, (Issued on Nov 12, 2021).

²⁸ *Id.*

²⁹ Reserve Bank of India, Guidelines on Storage of Payment Data, RBI/2017-18/153 DPSS.CO.OD No.2785/06.08.005/2017-2018, (Issued on Apr 6, 2018),

³⁰ *Id.*

³¹ The Income Tax Act, § 131, No 43, Acts of Parliament, 1961 (India).

³² *Shankarlal Agarwalla v. State Bank of India And Anr*, AIR 1987 Cal 29.

B. LIABILITY TOWARDS REGULATORY AUTHORITIES

Just as PAs are liable towards customer, there are also certain liabilities towards the Merchant. Escrow account management and settlement periods are perhaps the most crucial part of this relationship. It is understandable that defaults on the part of PA to settle up due amounts can result in major losses to the merchants. As evidenced from the guidelines, non-bank PAs are to maintain an escrow account where the funds are collected and later transferred to the merchant on a T_p+0 to T_p+1 basis.³³ The settlement period depends upon whether the merchant (T_d+1) [T_d' - date of confirmation by the merchant to the intermediary about delivery of goods to the customer.] or the PA (T_s+1) [T_s' - date of intimation by the merchant to the intermediary about shipment of goods] is responsible for the delivery of goods/services. The PAs are further able to facilitate all refund processes only via the escrow account unless otherwise agreed upon by the merchant and customer.

Apart from this, the PAs are, required to take on liability relating to customer management and grievance redressal as already discussed above. It becomes rather clear that by engaging the services of the PA, merchants are to a large extent absolved of substantial liability and duty towards the customers. With the PAs being responsible to ensure the authenticity and veracity of these online merchants, it appears that there is a great onus of liability that is being shifted from merchants to PAs. This in itself is an interesting position wherein an intermediary even with respect to ensuring that pay-outs are made timely, it is the duty of the escrow bank to ensure that these funds maintained are used solely for paying the merchants and not to issue loans etc.³⁴

All in law, the entire regulatory framework relating to PAs and their liability seems to be highly inter-linked and inter-related where liabilities of the various parties are affixed on one and another.

V. FINDINGS, SUGGESTIONS AND CONCLUSION

Undoubtedly, India has come a long way with respect to the adaptation and promotion of digital payment methodologies and other FinTech developments. The entire PA business was perhaps one of the most revolutionary inventions of all time that brought us closer to a modern, digitally friendly India. The introduction of Guidelines on Regulation of Payment Aggregators and

³³ *Supra* note 2.

³⁴ Reserve Bank of India, Master Directions on Prepaid Payment Instruments (PPIs), RBI/DPSS/2021-22/82, (updated on Feb 10, 2023).

Payment Gateways by the RBI was truly a revolutionary step and was one of the most critical steps towards a more digitally sound and secure India. The guidelines released in 2020 proved to be a positive step in the direction of establishing a clear framework for the operation of PAs and PGs and surely did open up avenues. The RBI citing concerns over the models of PAs and their operation pushed for these guidelines³⁵ The RBI has been extremely cautious while handing out these licenses to non-banking PAs and this has resulted in an increased number of pending applications³⁶

Considering the ease that PAs offer, more and more corporates are coming forward with their own PA systems to eliminate external third parties and to shorten the bridge between the merchants and customers.³⁷ This marks a new era of digital payments. Although the Payment aggregator guidelines released by the RBI read along with the PSSA Act is a commendable entry into the arena of online payment regulation, there is much scope for improvement.

From our detailed discussion through the course of this paper, there have been a few key takeaways.

Firstly, we were able to understand that PAs are a lot more complicated than traditional banks owing to the nature of transactions and the parties involved. We cannot compare the nature of a traditional bank to that of a PA although some of the functions are the same. Additionally, we were able to discuss the various guidelines and regulations in place with regards to such aggregators and a detailed reading of it suggests that while there is a significant improvement, there are several gaps that are to be filled and several nuances that enquire special attention. The government and the RBI ought to look into the complete functioning of such aggregators and come up with a legislation or bring it within the ambit of the Banking Regulations Act, 1949 to ensure maximum accountability and clarity. The existing norms though do suffice in terms of providing a general guidance, they lack clarity on several accounts such as intricacies of reporting, lack of fixed time frames, and confusion regarding the liability imposed. Interestingly enough, we were also able to identify that PAs do in fact have a high degree of

³⁵ Manojit Saha, *Payment platforms under RBI scrutiny*, BUSINESS STANDARD, (Mar 25, 2022), https://www.business-standard.com/article/economy-policy/data-breach-business-models-of-payment-platforms-under-rbi-scrutiny-122032401531_1.html.

³⁶ Arti Singh, *RBI returns a large number of payment aggregator license application*, (Jul 7, 2022), <https://www.livemint.com/industry/banking/why-rbi-is-wary-of-payment-aggregators-11657126296607.html>

³⁷ Ashwin Manikandan, *From Amazon to Zomato, a big crowd at RBI doors for payment aggregator licence*, (Aug 19, 2021) <https://economictimes.indiatimes.com/tech/technology/a-big-crowd-at-rbi-doors-for-payment-aggregator-licence/articleshow/85439562.cms>.

liability imposed on them both from the regulatory bodies and from the merchants and are more or less responsible for ensuring authenticity of merchants, compliance, and to ensure that merchants are not engaged in any sort of fraudulent or suspicious activity. PAs have a very robust and vibrant future ahead of them and can completely revolutionize the online payment scene.

In terms of what can be done with regards to the existing condition relating to the PA system, there are a few suggestions.

1. The possibility of creating a sub-committee or another statutory body such as Security Exchange Board of India ('SEBI') specifically for monitoring all aspects relating to the functioning, compliance and reporting of PAs and all PAs would be required to directly comply with and report to these bodies on a periodic basis and the body in turn will report to RBI its findings. At present, the RBI has far too much under its authority.
2. There is a need for the Regulators to promote a cooperative reporting system between banks, merchants and PAs to provide complied reports of risk assessment, safety measures and performance.
3. There is a need for the regulatory bodies to come up with a set of security risks, payment issues, and other problems that may arise in the course of conducting such PA business and ensure that this is publicly available to all banks, PAs and merchants along with the customers.
4. Instead of imposing the liability of compliance on part of PAs on the banks, there could be devised a scenario where the new proposed regulatory body would be in charge of ensuring such compliance and further penalising any individuals found in violation. Furthermore, instead of asking PAs to verify the authenticity of merchants, similar to the PA license system, there may exist a Merchant license system as well. Only upon the receipt of such a license will merchants be allowed to carry out such online businesses and undertake the services offered by PAs. Only merchants with valid licences shall be permitted to engage the services offered by PAs

PAs have no doubt had a major impact on the banking sector of India and has revolutionised the way merchants and customers transact. As the banking systems evolve, there is a need for the relevant laws and guidelines to accommodate this change in technology. India has always managed to remain on top of technology but every once in a while, there is bound to be a gap and that just so happens to be the case with PAs. While the guidelines issued

by the RBI appear to be a great step in the right direction, there are several concerns that are yet to be addressed. We see that it is not just the private entities but also government undertakings such as Indian Railway Catering and Tourism Corporation ('IRCTC') entering the market of the payment aggregation business.³⁸

The upcoming years will see a boom in the online payment and PA business and when such a boom does come about, it is essential that the government, merchants, customers and the entities themselves remain prepared. By filling the existing gaps in the framework and through a system of constant monitoring and reporting, we will be able to ensure that our system is up to date with all the changes and hence is strong enough to withstand any challenge that may come about. Until then, there is a need for increased caution and compliance on part of all the parties engaged in such transactions.

³⁸ Dhruvaksh Saha, *Payment aggregator licence may open avenues beyond rail-ticketing for IRCTC*, BUSINESS STANDARD, (Sept 19, 2022), https://www.business-standard.com/article/companies/payment-aggregator-licence-may-open-avenues-beyond-rail-ticketing-for-irctc-122091900694_1.html.