INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

A COMPREHENSIVE STUDY ON RBI AND SEBI REGULATIONS IMPACTING NON-BANKING E-COMMERCE SERVICES

AUTHORED BY - AMOLIKA ROY

Designation: Master Student of Cyber Law Information Security National Law Institute University, Bhopal

Abstract

This study delves into the prevalent non-compliances with RBI and SEBI guidelines in the non-banking e-commerce services domain, shedding light on issues like delayed transaction processing, inadequate fraud prevention mechanisms, and dissemination of misleading information. By examining cases such as Saristha Devi v. State Bank of India and responses from entities like Razorpay Software Private Limited, the repercussions of flouting regulatory norms are analyzed. Moreover, the paper deliberates on the regulatory ambiguity surrounding payment aggregators like Amazon Pay and Airtel Pay, along with the emergence of neobanks.

To address these challenges, the adoption of blockchain technology and adherence to best practices are proposed to bolster security, streamline compliance procedures, and encourage innovation. Recommendations entail advocating for equitable access to payment infrastructure, investing in fintech solutions for cybersecurity and fraud deterrence, and fostering cooperation with regulatory authorities to navigate the regulatory framework adeptly.

Ultimately, rectifying these non-compliances and ensuring alignment with RBI and SEBI regulations are imperative for nurturing consumer confidence, bolstering financial stability, and fostering the expansion of non-banking e-commerce services in India.

Keywords: non-banking e-commerce services, RBI, SEBI, compliance, payment aggregators, fraud prevention, cybersecurity, regulatory framework, blockchain technology, neobanks, fintech, innovation, consumer trust, financial stability, India.

Introduction

In the dynamic realm of digital payments and non-banking e-commerce, adherence to regulations set forth by authorities like the Reserve Bank of India (RBI) and Securities and Exchange Board of India (SEBI) is paramount. These regulations are designed to safeguard consumers, uphold the integrity of the financial system, and foster innovation while ensuring legal compliance. Nonetheless, the non-banking e-commerce sector often grapples with meeting these standards, leading to challenges such as transaction delays, inadequate fraud protection, and misinformation dissemination.

One significant area of concern lies in the adherence of payment aggregators to RBI and SEBI regulations. These aggregators facilitate online transactions but occasionally fall short of the stringent regulatory requirements. For instance, instances like Saristha Devi v. State Bank of India highlight issues such as delayed refunds and deficient communication, prompting legal recourse. Similarly, incidents involving entities like Razorpay Software Private Limited underscore the necessity for robust fraud prevention mechanisms and strict adherence to regulatory guidelines.

Furthermore, the classification of payment aggregators like Amazon Pay and Airtel Pay poses challenges in aligning with the appropriate regulatory frameworks and delineating boundaries with Non-Banking Financial Companies (NBFCs). The emergence of neobanks, operating exclusively in the digital domain, further complicates regulatory oversight as they offer a range of financial services online.

To surmount these hurdles, the non-banking e-commerce sector should embrace blockchain technology and adopt best practices to bolster security, streamline compliance procedures, and foster innovation. Leveraging blockchain's transparent ledger system and advocating for equitable access to payment infrastructure can enhance regulatory compliance, instill consumer confidence, and promote financial stability. Collaborating with regulators and investing in fintech solutions for cybersecurity and fraud prevention are imperative steps to meet regulatory obligations and thrive in the digital payments landscape.

Literature Review

1. **Srivastava A, Srivastava A and Maheshwari R, 'Fintech Laws and Regulations: India:GLI' (*GLI - Global Legal Insights - International legal business solutions*, 12 September 2023) <https://www.globallegalinsights.com/practice-areas/fintech-**

laws-and-regulations/india> accessed 8 March 2024 In India, the fintech sector is booming with digital payments and lending leading the way. Government initiatives like Startup India and demonetization, along with RBI's regulations and innovations like UPI Lite, support this growth. Wealthtech and Insurtech sectors are expanding rapidly, while the VDA industry awaits comprehensive regulation. Regulatory bodies like RBI, SEBI, and IRDAI oversee different aspects, ensuring transparency and compliance. Cross-border initiatives aim to enhance payment efficiency and connectivity.

2. **Zaveri B, 'Open Questions on RBI's Enforcement Actions in Indian Fintech' (*IndiaCorpLaw*, 22 February 2024) <https://indiacorplaw.in/2024/02/open-questions-on-rbis-enforcement-actions-in-indian-fintech.html> accessed 8 March 2024.** The article highlights the ambiguity surrounding the classification of certain intermediaries involved in payment aggregation, questioning whether they qualify as payment systems under the PSS Act. It underscores the need for clarity in defining such arrangements and their regulatory implications, particularly in the context of RBI's enforcement actions in the Indian fintech sector.

3. **Ahluwalia S, Malhotra H and Anand P, 'Fintech 2023 Comparisons' (*Comparisons | Global Practice Guides | Chambers and Partners*) <https://practiceguides.chambers.com/practice-guides/comparison/768/10598/17027-17029-17043-17047-17052-17055-17058-17068-17073-17077-17080-17083-17093> accessed 8 March 2024** The article outlines India's fintech sector growth and regulatory updates, including developments in payment aggregators. It highlights their role in facilitating online transactions and the RBI's regulations mandating licensing and technical standards compliance. The piece emphasizes adherence to RBI guidelines within the broader fintech regulatory framework.

4. **Gupta D and Tandon S, 'RBI Framework for Cross-Border Payment Aggregators: A Shift in Regulatory Approach' (*Legal Developments*, 5 December 2023) <https://www.legal500.com/developments/thought-leadership/rbi-framework-for-cross-border-payment-aggregators-a-shift-in-regulatory-approach/> accessed 8 March 2024** The article discusses about how RBI introduced the Payment Aggregator - Cross Border (PA-CB) Framework in October 2023 to regulate entities facilitating cross-border payment transactions for import and export of goods and services. It mandates authorisation from the RBI for such activities, with specific criteria for net worth and categories of PA-CB. The framework aims to enhance security and

transparency in cross-border payments while bringing all relevant entities under direct regulation.

5. **Jagannath J, 'RBI Imposes Penalty of Rs 3.06 Crore on Amazon Pay (India) for Violation of Norms' (*Business Today,* 3 March 2023) <https://www.businesstoday.in/latest/corporate/story/rbi-imposes-penalty-of-rs-306-crore-on-amazon-pay-india-heres-why-372179-2023-03-03> accessed 8 March 2024** The Reserve Bank of India (RBI) has fined Amazon Pay (India) Private Limited Rs 3.06 crore for breaching regulations on prepaid payment instruments and Know Your Customer (KYC) rules. Amazon Pay, recently licensed as a payment aggregator, was found non-compliant with RBI directives. The penalty, imposed under the Payment and Settlement Systems Act, 2007, reflects regulatory deficiencies. Amazon asserts its commitment to regulatory compliance and cooperation with authorities,

6. **Parasher S and Mehul , 'What Happened When the RBI Cancelled Payment Aggregator Licences?' (*StartupNews.fyi,* 3 February 2024) <https://startupnews.fyi/2024/02/03/what-happened-when-the-rbi-cancelled-payment-aggregator-licences/> accessed 8 March 2024** The article discusses the RBI's rejection of payment aggregator license applications, notably affecting Instamojo and other startups. Over 70 entities faced rejection, leading to operational halts and customer payment issues. Instamojo shut its PA business, impacting millions of merchants. Critics highlight RBI's lack of transparency and the need for smoother transitions post-orders. The central bank's actions raise concerns about consumer protection and regulatory efficacy.

7. **Panda S and Mahalik J, 'Regulatory Dynamics and Operational Impacts: Navigating India's Fin-Tech Landscape with the Latest Payment Aggregator Cross-Border Guidelines' (*CBCL,* 29 December 2023) <https://cbcl.nliu.ac.in/banking-law/regulatory-dynamics-and-operational-impacts-navigating-indias-fin-tech-landscape-with-the-latest-payment-aggregator-cross-border-guidelines/> accessed 9 March 2024** India's Fin-tech sector is undergoing significant regulatory changes aimed at securing cross-border transactions and protecting consumer rights. The Reserve Bank of India (RBI) has introduced new guidelines requiring non-bank entities to obtain authorization for cross-border payment services. While these regulations enhance transparency and security, they also pose compliance challenges for Fin-tech startups. Balancing regulatory oversight and fostering innovation is crucial for navigating India's evolving fintech landscape.

Statement of problem

Unclear regulatory classifications and enforcement actions in India's fintech sector create ambiguity and compliance challenges for payment aggregators and startups.

Hypothesis

Clearer regulatory framework and efficient enforcement actions in India's fintech sector will improve compliance and foster innovation among payment aggregators and other non-banking ecommerce entities.

Research questions

- How do regulatory changes impact the operational efficiency of payment aggregators, non-banking financial companies in India?
- How can fintech companies navigate the balance between regulatory compliance and innovation in India's evolving regulatory landscape? (emerging concept of neobanks)
- How do regulatory actions, such as license rejections or penalties, affect the viability and sustainability of payment aggregator businesses in India?
- How can regulatory bodies enhance transparency and consumer protection while fostering innovation in India's fintech ecommerce landscape?
- What specific RBI and SEBI regulations impact non-banking e-commerce services like Amazon Pay and Airtel Pay?

Research objectives

- To examine the impact of regulatory changes on the operational efficiency of payment aggregators and non-banking financial companies in India, with a focus on identifying challenges and opportunities for these entities.
- To investigate strategies and approaches employed by fintech companies to effectively balance regulatory compliance and innovation in India's evolving regulatory landscape, particularly in the context of emerging neobanks.
- To assess the effects of regulatory actions, such as license rejections or penalties, on the viability and sustainability of payment aggregator businesses in India, and to identify mitigation measures and best practices for regulatory compliance.

- To explore mechanisms through which regulatory bodies can enhance transparency and consumer protection while fostering innovation in India's fintech e-commerce landscape, aiming to promote a conducive environment for both businesses and consumers.
- To analyze specific RBI and SEBI regulations impacting non-banking e-commerce services like Amazon Pay and Airtel Pay, aiming to provide insights into compliance requirements and regulatory challenges faced by these service providers.

Scope and Limitation

The research project scope is limited to the analysis of payment aggregator non-conformity cases, Amazon Pay and Airtel Payment differences, and explores NBFCs and neobanks.

Research Methodology

The research methodology used for the research paper titled –'A Comprehensive Study on RBI and SEBI Regulations Impacting non-banking E-commerce Services (case study: amazon pay, Airtel pay)' is doctrinal methodology.

Analysis

Major Non-Conformities with RBI and SEBI Guidelines.

- In the context of regulatory guidelines set by authorities such as the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI), payment aggregators are expected to adhere to strict standards to safeguard the interests of consumers and maintain the integrity of the financial system. RBI guidelines mandate payment aggregators[1] to ensure prompt resolution of customer complaints, timely processing of transactions, and compliance with anti-money laundering and cybersecurity protocols[2]. Many times, the

[1] Section 1.1.1 of Guidelines on Regulation of Payment Aggregators and Payment Gateways **(**DPSS.CO.PD.No.1810/02.14.008/2019-20 dated March 17, 2020)
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. < https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11822>
Accessed on 02.03.2024

[2] Section 6. **Safeguards against Money Laundering (KYC / AML / CFT) Provisions**
6.1. The Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) guidelines issued by the Department of Regulation, RBI, in their "Master Direction – Know Your Customer (KYC) Directions" updated from time to time, shall apply mutatis mutandis to all entities.
6.2. Provisions of Prevention of Money Laundering Act, 2002 and Rules framed thereunder, as amended from time to time, shall also be applicable. < https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11822>
Accessed on 02.03.2024

payment aggregators fail to be compliant with such guidelines and faces consequences given in Chapter 7 of PSS act. One of such cases is ***Saristha Devi v. State Bank of India***[3]. The case involves a complaint filed by Saristha Devi against the State Bank of India (SBI) and Airtel DTH services regarding the non-crediting of a payment made for DTH recharge through internet banking. Saristha Devi's husband transferred an amount of Rs. 2652/- through SBI's internet banking facility to recharge their Airtel DTH account on April 21, 2020. However, despite the amount being debited from their account, it was not credited to their DTH account.Despite multiple complaints lodged by Saristha Devi's husband and subsequent responses from SBI stating that the transaction was successful, the amount was not credited to the DTH account. It was only later revealed through email correspondence that the intermediary payment aggregator, Oxygen Services India Private Limited, had processed a reversal of the transaction on March 31, 2022, and refunded the amount to SBI. The amount was then credited to Saristha Devi's husband's account on April 22, 2022, after almost two years. The Consumer Disputes Redressal Commission [4]found that the delay in refunding the amount, lack of communication regarding the reversal of the transaction, and incomplete information provided by SBI constituted deficiency in service. Despite SBI's claims of the transaction being successful, the Commission held them responsible for not providing timely and accurate information to Saristha Devi and her husband. Additionally, Airtel DTH services were also held liable for failing to address the complaint and for the harassment suffered by the complainant. As a result, the Commission ordered SBI and Airtel DTH services to jointly and severally pay compensation of Rs. 20,000/- to Saristha Devi and litigation costs of Rs. 5,000/- each. The case highlights the importance of payment aggregators in online transactions and the responsibilities of banks and service providers to ensure timely and accurate processing of payments.

- Another major aspect that PA are found non-compliant with is in ensuring security and safeguard from fraud and related activities. In ensuring the integrity and security of payment systems, Payment Aggregators (PAs) play a critical role by implementing robust risk management systems. Section 10 of the Security, Fraud Prevention, and Risk Management Framework outlines key mandates for PAs to adhere to. Notably, subsection

[3] *Saristha Devi Versus State Bank of India 29112023* <https://www.casemine.com/judgement/in/657199646d26c8429e2cb1d2> Accessed on 02.03.2024

[4] The National Consumer Disputes Redressal Commission (NCDRC) was established in 1988 under the Consumer Protection Act of 1986. Headquartered in New Delhi, it's led by a retired Judge of the Supreme Court or a Chief Justice of a High Court. It has jurisdiction over complaints valued over two crore and can hear appeals from State Commissions or District Fora. Appeals against NCDRC orders can be made to the Supreme Court within 30 days. <*National Consumer Disputes Redressal Commission*) <https://ncdrc.nic.in/history.html> Accessed on 02.03.2024

10.1 underscores the imperative of establishing a strong risk management system to address the evolving challenges of fraud while safeguarding customer interests. PAs are required to deploy adequate information and data security infrastructure and systems to prevent and detect fraudulent activities effectively. Furthermore, subsection 10.2 emphasizes the necessity for PAs to formulate a Board-approved information security policy, aligning with industry best practices, to ensure the safety and security of the payment systems they operate. Related case [5]happened in the case at hand revolves around the actions taken by a Payment Aggregator (PA), Razorpay Software Private Limited, in response to suspicious activities involving certain merchants who utilized its payment gateway services.

The petitioner, Razorpay, operates as a facilitator for online transactions, allowing businesses to accept various payment methods from customers without the need for merchants to create their own payment integration systems. The merchants involved in the case, including XY Data Steam Technology Private Limited, Super Data Sandbox Technology Private Limited, Flexbees India Technology Private Limited, Kortis Engineering Private Limited, and Fureins Technology Private Limited, availed Razorpay's services to accept payments through their online platforms. However, Razorpay's internal risk monitoring team detected suspicious activities associated with these merchants' accounts, prompting the company to disable their access to the payment gateway and freeze the funds held in their respective accounts. This action was taken to prevent any further fraudulent[6] transactions and to safeguard the funds of legitimate customers. The total amount frozen in the accounts of these merchants was Rs.1,62,25,778.35. Subsequently, a complaint was filed against the accused merchants for alleged online fraud, leading to the initiation of legal proceedings. Despite Razorpay not being named as an accused party in the complaint, authorities issued a notice under Section 91 of the Criminal Procedure Code (CrPC)[7], directing Razorpay to freeze additional funds totaling Rs.4,66,60,000.00, purportedly linked to the fraudulent activities of the merchants.

---

[5]*RAZORPAY SOFTWARE PRIVATE LIMITED vs THE STATE OF KARNATAKA AND ANR Karnataka High Court* (https://www.casemine.com/judgement/in/632fe29a66c77f7b4ff2fbb4)

[6] Section 25 IPC Fraudulent: A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise. (*India code: Indian penal code, 1860*) https://www.indiacode.nic.in/handle/123456789/2263?sam_handle=123456789/1362 accessed 09.03.2024

[7] Section 91. Summons to produce document or other thing. —
(*1*) Whenever any Court or any officer in
charge of a police station considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or such officer a written order, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it, or to produce it, at the time and place stated in the summons or order.

Razorpay, through its legal representatives, challenged the validity of the action taken by the authorities to freeze the additional funds beyond the amount initially blocked by the company. The petitioner argued that it had already taken appropriate measures by blocking the funds related to the accused merchants' transactions and that any further freezing of funds was unwarranted and constituted an abuse of legal process.

The High Court Government Pleader, representing the authorities, contended that Razorpay, as a payment aggregator, should have detected and prevented the fraudulent activities facilitated through its platform. Therefore, the authorities justified their actions in freezing the additional funds associated with the accused merchants' transactions.The court's deliberations focused on determining the legality of the authorities' actions in freezing the funds held by Razorpay beyond the amount initially blocked by the company. The court considered relevant regulations issued by the Reserve Bank of India (RBI), which govern the activities of payment aggregators and payment gateways, and examined whether Razorpay had fulfilled its regulatory obligations.

- Another major important aspect that is to be taken care of by the payment aggregator is to adhere to Section 11(2)(ia) and 11C(3) of the SEBI Act, 1992[8] which talks about the powers vested in SEBI and its Investigating Authority to gather information, conduct inquiries, and investigate matters related to the securities market, ensuring regulatory compliance and market integrity. Case regarding this issue is seen in ***THE SECURITIES AND EXCHANGE BOARD OF***

(*2*) Any person required under this section merely to produce a document or other thing shall be deemed to have complied with the requisition if he causes such document or thing to be produced instead of attending personally to produce the same.
(*3*) Nothing in this section shall be deemed—
(*a*) to affect sections 123 and 124 of the Indian Evidence Act, 1872 (1 of 1872), or the Bankers' Books Evidence Act, 1891 (13 of 1891), or
(*b*) to apply to a letter, postcard, telegram or other document or any parcel or thing in the custody of the postal or telegraph authority. (*The code of criminal procedure, 1973*) https://www.indiacode.nic.in/bitstream/123456789/15272/1/the_code_of_criminal_procedure,_1973.pdf accessed 04.03.2024

[8] Section 11(2)(i) is on calling for information from, undertaking inspection, conducting inquiries and audits of the stock exchange and mutual funds, other persons associated with the securities market intermediaries and self regulatory organizations on the securities market. This power is not available to be exercised in an investigation. The summons issued by the "Investigating Officer" clearly states that it is "in connection with the investigation instituted by SEBI." Section 11(2)(ia) is on calling for information and record from any bank or any other authority or board or corporation established or constituted by or under any Central, State or Provincial Act in respect of any transactions in securities, which is under investigation or inquiry by the Board. Power under 11(2)(ia) is also not available to issue summons to the Appellant as the Appellant is not one of the entities specified therein.
It is further submitted that since the scope and reach of section 11(3) was not adequate to meet the requirements in an investigation, new section 11C captioned "Investigation" was included in the Act, through the amendment brought into force with effect from 29.10.2002. Summons referred to in the impugned order is under section 11(3). For failure to comply with the requirements of section 11C penalty has been provided in the said section itself and the offence cannot be adjudicated by the Adjudicating Officer under section 15 I. (*Securities and Exchange Board of India*) <https://www.sebi.gov.in/sebi_data/docfiles/11466_t.html> Accessed 05.03.2024

INDIA vs Quadrant Televentures Limited.The adjudication order pertains to Quadrant Televentures Limited (formerly known as HFCL Infotel Limited) in the matter of providing incorrect, incomplete, contradictory, and misleading information to the Investigating Authority, which resulted in violations of Section 11(2)(ia) and 11C(3) of the SEBI Act, 1992.[9]

In summary, the violations relate to the following:

1. Failure to furnish complete and accurate information in response to summonses issued by the Investigating Authority.
2. Providing contradictory answers and incomplete information regarding transactions, customer application forms, and payment details.
3. Non-compliance with requests for relevant documents, such as bank statements.
4. Misleading responses regarding the rates charged per SMS and the involvement of aggregators.

The order imposes a penalty of Rs. 2,00,000/- (Rupees Two Lakhs) under Section 15A(a) of the SEBI Act, 1992. The Noticee is directed to remit/pay the penalty amount within 45 days of receiving the order. Failure to comply may result in further enforcement proceedings, including recovery proceedings under Section 28A of the SEBI Act.

The Noticee is also instructed to provide confirmation of payment to the Enforcement Department of SEBI, failing which, recovery proceedings may be initiated.The violations mentioned in the order pertain to providing misleading information and non-compliance with the Investigating Authority's requests, particularly regarding transactions, customer application forms, payment details, and rates charged per SMS.

- Guidelines on Regulation of Payment Aggregators and Payment Gateways[10] made with respect to PSS Act specifically talks about payment aggregators and payment gateways but clause

[9] Using a Payment Application Data Security Standard (PA-DSS) compliant application alone doesn't ensure Payment Card Industry Data Security Standard (PCI DSS) compliance. The application must be integrated into a PCI DSS compliant environment as per the vendor's PA-DSS Implementation Guide. While vendors themselves may not be directly subject to PCI DSS, their applications must support customers' PCI DSS compliance. Insecure payment applications can hinder compliance by storing sensitive data improperly, requiring disabling of security features, or using insecure support methods. Secure payment applications, within a PCI DSS-compliant setup, help minimize security breaches and associated fraud risks. (*Payment application data security standard*) https://www.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf accessed 05.03.2024.

[10] Section 1.1.2. of Guidelines on Regulation of Payment Aggregators and Payment Gateways PGs are entities that provide technology infrastructure to route and facilitate processing of an online payment transaction without any

7.3 and 7.4 of the guidelines present a contradiction regarding the responsibility of payment aggregators and merchants[11] in ensuring compliance with PCI-DSS and PA-DSS standards. While clause 7.3 places the responsibility on payment aggregators to check compliance, clause 7.4 prohibits merchants from saving card-related data, implying minimal involvement on their part. This contradiction raises confusion about the necessity for merchants to adhere to these standards if they cannot store such data.

Moreover, imposing PCI-DSS and PA-DSS [12]compliance requirements may disproportionately burden small businesses like sole proprietorships and MSMEs. These entities may struggle to meet the stringent standards, potentially hindering their ability to conduct online transactions effectively. Balancing security requirements with the operational capacities of smaller businesses is crucial to ensuring equitable access to online payment modes.

Amazon pay and airtel pay banking ecommerce services similar yet different.
Airtel Payments Bank has been designated as a *scheduled bank*[13] by the RBI, allowing it to pursue government contracts and welfare schemes. With a user base of 115 million, it turned profitable in September 2021. Offering a range of digital solutions through its app and extensive retail network, it emphasizes quick and secure account opening, digital savings programs, and safe payment options like Airtel Safe Pay.[14] Although in recent past years airtel payments have been fined heavily due to non-compliance with guidelines issued as of on March 7, 2018, the Reserve Bank of India (RBI) imposed a ₹50 million penalty on Airtel Payments Bank Limited[15] for violating the 'Operating Guidelines for Payments Banks' and RBI's directives on Know Your Customer (KYC) norms. This action was taken under Section 47A(1)(c) read with Section 46(4)(i) of the Banking Regulation Act, 1949. The penalty stemmed from complaints and media reports

involvement in handling of funds. (*Reserve Bank of India Notification)* < https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11822> Accessed on 02.03.2024

[11] A merchant account, essentially a business bank account, allows companies to receive payments, particularly through credit or debit cards. Partnering with an acquiring bank or provider facilitates electronic transactions, with funds typically transferred within 3 to 5 days, though some offer same-day transfers. Sandeep G, "What Is a Merchant Account? How Account Processing Works?" (*Razorpay Blog*, February 13, 2024) https://razorpay.com/blog/what-is-merchant-account/ accessed on 05.03.2024

[13] Scheduled Commercial Banks in India are categorised into five different groups according to their ownership and / or nature of operation. These bank groups are (i) State Bank of India and its Associates, (ii) Nationalised Banks, (iii) Private Sector Banks, (iv) Foreign Banks, and (v) Regional Rural Banks. In the bank group-wise classification, IDBI Bank Ltd. has been included in Nationalised Banks. "Explanatory Notes I. Bank-Related" (November 8, 2012) https://www.rbi.org.in/scripts/PublicationsView.aspx?id=14655 accessed March 6, 2024

[14]"Inclusion of 'Airtel Payments Bank Limited' in the Second Schedule of the Reserve Bank of India Act, 1934" (January 7, 2020) https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12217&Mode=0 accessed March 6, 2024

[15] "Reserve Bank of India" https://www.rbi.org.in/commonperson/english/scripts/PressReleases.aspx?Id=2541 accessed on 05.03.2024

alleging unauthorized customer account openings. Following a supervisory visit in November 2017 and subsequent investigations, RBI found the bank in contravention of its guidelines. Despite the bank's response, RBI deemed the charges substantiated, leading to the imposition of the penalty.

There might be instances where amazon pay like services and airtel payment services may seem to be similar yet they are different are need to comply with respective regulation that are made according to the category they are recognized under.

The recent authorizations by the RBI to entities like Amazon Pay, Stripe, Juspay, Tata Payments, and MSwipe as *payment aggregators* have sparked confusion in the financial sector. While these entities are categorized as payment aggregators, they also possess the capability to offer lending services. This blurs the line between payment aggregators and Non-Banking Financial Companies (NBFCs), creating ambiguity for regulatory compliance. Despite clear distinctions between banks and NBFCs[16], the overlapping services offered by payment aggregators raise challenges in understanding their regulatory classification and adhering to relevant regulations.

[16] A Non-Banking Financial Company (NBFC) is a registered entity under the Companies Act, 1956, engaged in various financial activities like lending, investments, leasing, and insurance. However, it does not include institutions primarily involved in agricultural or industrial activities, sale of goods, or real estate transactions. Additionally, if an NBFC's primary business involves receiving deposits from the public, it's termed as a Residuary NBFC. "All You Wanted to Know about NBFCs" (January 10, 2017) https://www.rbi.org.in/commonperson/english/scripts/FAQs.aspx?Id=1167 accessed March 6, 2024

ANNEX-I

CHART - I

Overview of Regulators of Non-Banking Companies

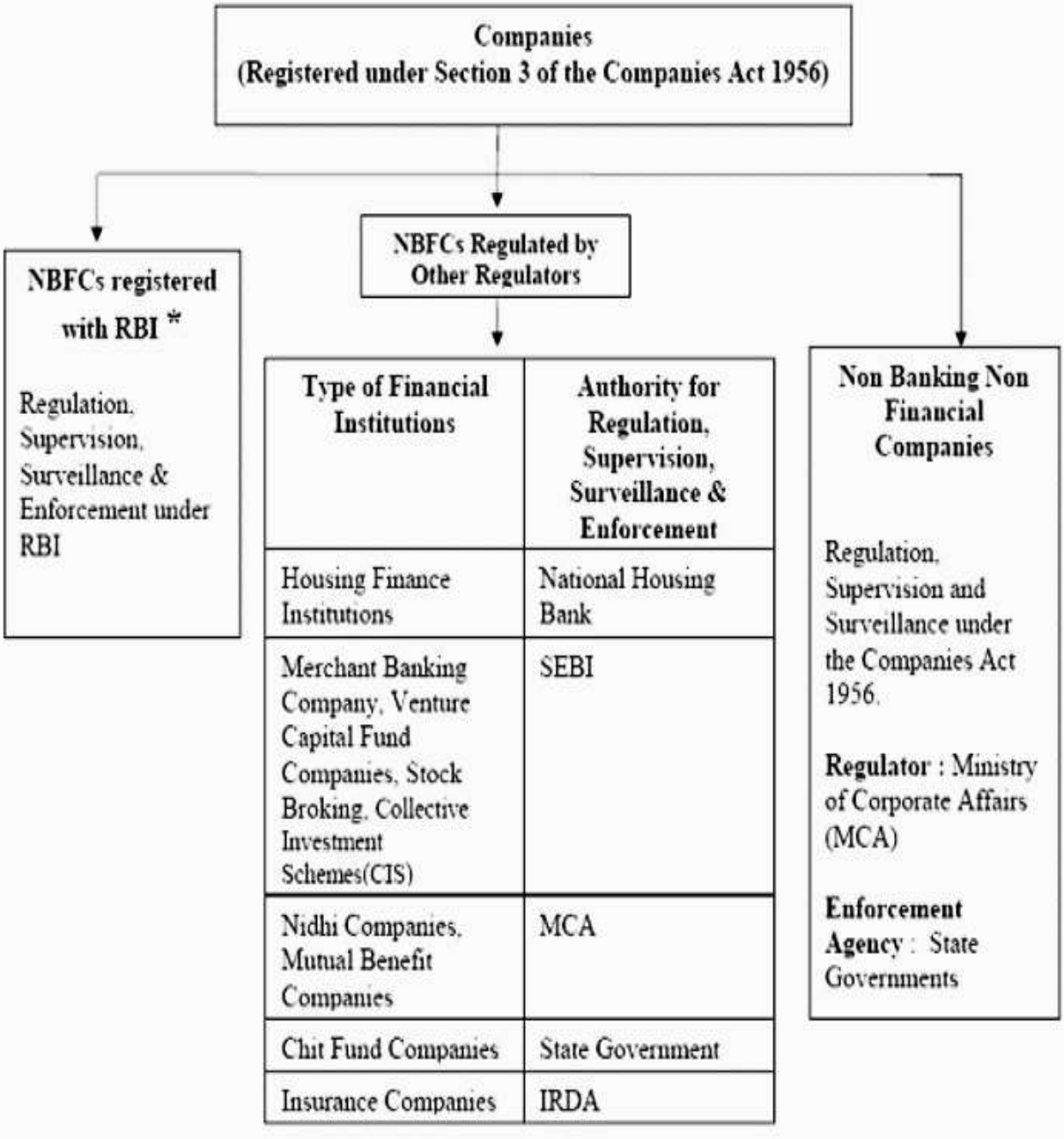

Fig : 1 Regulators of Non-Banking companies under section 3 of Companies Act 1956

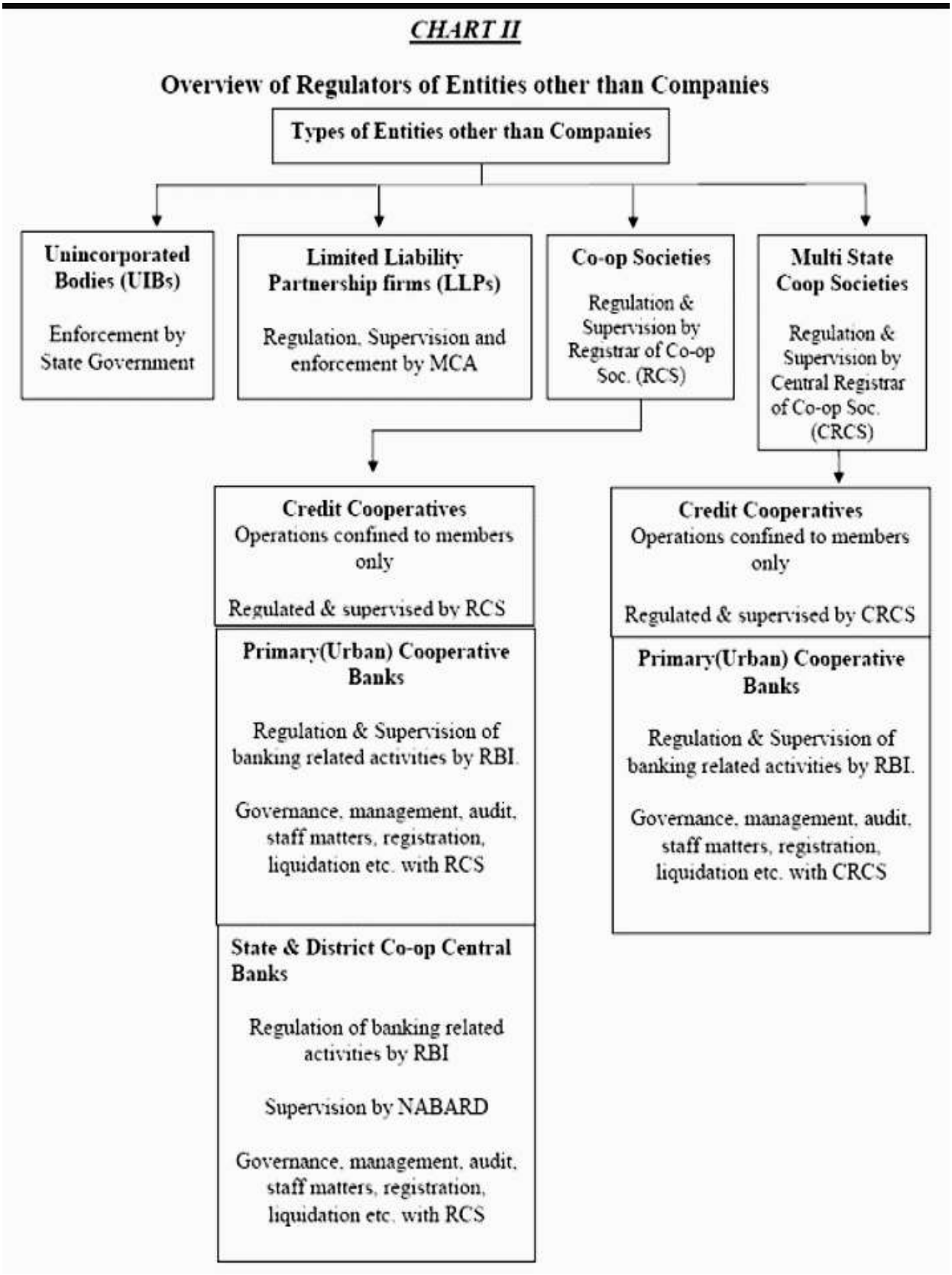

Fig : 2 Regulators of Non-Banking entities other than companies

The Non-Banking Finance Company (NBFC) sector has experienced significant growth and complexity over time, necessitating a robust IT framework to ensure safety, security, and efficiency in operations. To address this, regulatory directions have been issued, outlining comprehensive guidelines for IT governance, policy formulation, information and cyber security, IT operations, IS audit, business continuity planning, and IT services outsourcing.

Key aspects of the proposed IT framework include establishing clear IT governance structures, formulating board-approved IT policies, enhancing information and cyber security measures, ensuring robust IT operations, conducting regular IS audits, and implementing effective business continuity planning and disaster recovery strategies.

For NBFCs with assets above ₹ 500 crore, the framework emphasizes the formation of an IT Strategy Committee, development of comprehensive IT policies, implementation of advanced security measures, adoption of sound business continuity practices, and meticulous oversight of IT services outsourcing.

For smaller NBFCs with assets below ₹ 500 crore, the recommendations focus on establishing basic IT systems with fundamental security measures, ensuring regulatory compliance, implementing basic cyber security measures, and developing a board-approved BCP policy.

In essence, the proposed IT framework aims to align the NBFC sector's IT practices with industry best practices, enhancing resilience, efficiency, and security across all operations. Compliance timelines have been provided, urging NBFCs to conduct gap analyses, develop action plans, and ensure full compliance within stipulated timelines.[17]

Emerging concept of Neo-banks

In jurisdictions where neobanks operate, the regulations usually don't mandate them to have physical branches. Consequently, neobanks function entirely through digital platforms, without the need for physical locations. These digital banks, often referred to as neobanks, leverage technology to offer banking services exclusively online, catering to customers' financial needs without traditional brick-and-mortar branches. Unlike traditional banks, neobanks operate solely in the digital realm, providing a range of banking services through mobile apps and online platforms.

[17]"Master Direction - Information Technology Framework for the NBFC Sector" (June 8, 2017) https://m.rbi.org.in//scripts/bs_viewmasdirections.aspx?id=10999 accessed March 6, 2024

Neobanks[18] offer a variety of financial products and services that fall under the purview of different regulators, including the RBI, SEBI, and IRDAI. Depending on the nature of the product or service and the role of the neobank, they may need to obtain licenses or approvals from the relevant regulator. This requirement varies based on whether the neobank partners with existing financial institutions or operates independently.

For areas where direct regulatory oversight doesn't apply, neobanks are subject to outsourcing and business correspondent guidelines issued by the respective regulators. These guidelines govern activities such as engaging business correspondents, outsourcing payment and settlement-related activities, managing risks, and ensuring code of conduct compliance.

The regulations indirectly affect neobanks through contractual agreements with their regulated partners. Neobanks enter into legal agreements with various regulated entities to provide a range of products and services. These agreements outline the terms and conditions governing the provision of financial services, ensuring compliance with regulatory requirements Neobanks, due to their business model, have access to significant customer data, either independently or through partnerships with financial institutions. It's crucial for neobanks to handle this data appropriately, following strict security standards to ensure its confidentiality and integrity. Currently, neobanks already adhere to various technical standards like ISO 27701 and PCI-DSS to protect customer data, alongside standards imposed by regulated entities.

Recent remarks by RBI Deputy Governor M. Rajeshwar Rao emphasized the importance of robust data protection and privacy laws before widespread adoption of open banking frameworks. India has taken steps in this direction with the introduction of The Digital Personal Data Protection act 2023, in Parliament. This act aims to safeguard individual personal data and establish a data protection authority. Neobanks will need to consider the provisions of this act when accessing, storing, and sharing customer data.

Conclusion

In conclusion, the analysis reveals significant non-conformities with RBI and SEBI regulations within the non-banking e-commerce services sector, exemplified by cases of delayed transaction processing, inadequate fraud prevention measures, and misleading information provision. These

18

instances underscore the importance of payment aggregators adhering to strict standards to safeguard consumer interests and maintain financial system integrity.

Furthermore, the ambiguity surrounding the regulatory classification of payment aggregators, such as Amazon Pay and Airtel Pay, raises concerns about compliance with respective guidelines and the potential blurring of lines between payment aggregators and NBFCs. Clearer regulatory frameworks are needed to ensure accountability and adherence to relevant regulations in this evolving landscape.

The proposed IT framework for NBFCs aims to enhance safety, security, and efficiency in operations through robust governance structures, policy formulation, and cybersecurity measures. However, challenges remain in implementing these guidelines, particularly for smaller NBFCs with limited resources.

Addressing these non-conformities and ensuring compliance with RBI and SEBI regulations is crucial for fostering consumer trust, promoting financial stability, and facilitating the growth of non-banking e-commerce services in India.

Suggestion

Implementation of blockchain

1. **Enhanced Security and Fraud Prevention**: Implement blockchain-based systems to enhance security and reduce fraud in digital transactions. Utilize smart contracts for automated payment processing, ensuring adherence to predefined conditions set by regulatory authorities. This not only reduces the risk of fraudulent activities but also ensures compliance with regulatory standards.
2. **Transparent Transaction Records**: Leverage blockchain's transparent ledger system to maintain accurate and auditable transaction records. By recording all transactions on a decentralized ledger, payment aggregators and e-commerce services can ensure transparency and accountability, aligning with regulatory requirements for transaction reporting and audit trails.
3. **Compliance Automation**: Utilize blockchain-based smart contracts to automate compliance processes and ensure adherence to regulatory guidelines. Smart contracts can be programmed to enforce regulatory requirements automatically, such as verifying

customer identities or ensuring compliance with transaction limits. This reduces manual intervention and minimizes the risk of regulatory non-compliance.

4 **Streamlined Cross-Border Transactions**: Blockchain technology enables faster and more cost-effective cross-border transactions by eliminating intermediaries and reducing transaction fees. Payment aggregators and e-commerce services can leverage blockchain-based platforms to streamline international payments while ensuring compliance with RBI guidelines on cross-border transactions and foreign exchange regulations.

5 **Data Privacy and Consent Management**: Utilize blockchain's cryptographic features to enhance data privacy and consent management. Implement decentralized identity solutions to give users greater control over their personal data and ensure compliance with data protection regulations such as GDPR. Blockchain-based identity management systems can enable secure and verifiable authentication processes, enhancing trust and compliance with regulatory standards.

6 **Regulatory Reporting and Auditing**: Utilize blockchain-based platforms to facilitate regulatory reporting and auditing processes. By maintaining a tamper-proof record of transactions on a decentralized ledger, payment aggregators and e-commerce services can simplify compliance reporting and provide auditors with transparent access to transaction data. This ensures compliance with regulatory requirements for reporting and auditing of financial transactions.

Implementing best practices

- To navigate the regulatory landscape and enhance competitiveness in the digital payment's ecosystem, e-commerce services such as Amazon Pay or Airtel Pay can focus on several key strategies. Firstly, advocating for non-discriminatory access to payment infrastructure is crucial. This involves urging regulatory bodies like RBI and NPCI [19]to ensure equal opportunities for both banks and non-bank financial firms, pushing for the reassessment of restrictions on non-bank access to payment systems like AEPS, and emphasizing the importance of competition and innovation through calibrated liberalization.

[19]NPCI, backed by RBI and Indian Banks' Association, pioneers retail payment systems in India. It offers diverse products like RuPay, IMPS, UPI, ensuring seamless electronic transactions, financial inclusion, and advancing India towards a cashless economy through innovative solutions like AePS and NETC. NPCI, it has been incorporated as a "Not for Profit" Company under the provisions of Section 25 of Companies Act 1956 (now Section 8 of Companies Act 2013) "An Introduction to NPCI and Its Various Products" https://www.npci.org.in/who-we-are/about-us accessed March 7, 2024

- Secondly, investing in fintech for enhanced cybersecurity[20] and fraud control is imperative. Recognizing the importance of fintech solutions in bolstering cybersecurity and fraud prevention, e-commerce services should advocate for the adoption of such innovations, particularly among non-bank financial service providers. Encouraging fintech firms specializing in these areas to establish operations in India and facilitating regulatory approvals for their expansion can further strengthen cybersecurity measures.
- Thirdly, collaborative efforts with regulatory bodies like RBI and SEBI are essential to foster innovation. By engaging in discussions and consultations, e-commerce services can provide insights into the specific regulatory challenges they face. Advocating for regulatory frameworks that support fintech adoption and innovation will create a conducive environment for growth while ensuring compliance with regulatory requirements.

Referecnes

- *Saristha Devi Versus State Bank of India 29112023* (https://www.casemine.com/judgement/in/657199646d26c8429e2cb1d2)
- *RAZORPAY SOFTWARE PRIVATE LIMITED vs THE STATE OF KARNATAKA AND ANR Karnataka High Court* (https://www.casemine.com/judgement/in/632fe29a66c77f7b4ff2fbb4)
- Chacko M and Hariramani A, 'A Critique of the Payment Gateways and Payment Aggregators Guidelines' (*SRL*, 27 February 2024) https://spiceroutelegal.com/publications/a-critique-of-the-payment-gateways-and-payment-aggregators-guidelines/ accessed 9 March 2024
- Ahluwalia S, Malhotra H and Anand P, 'Fintech 2023 Comparisons' (*Comparisons | Global Practice Guides | Chambers and Partners*) https://practiceguides.chambers.com/practice-guides/comparison/768/10598/17027-17029-17043-17047-17052-17055-17058-17068-17073-17077-17080-17083-17093 accessed 8 March 2024
- "The Evolution of Neobanks in India Impact on the Financial Ecosystem" (September 2021) https://www.pwc.in/industries/financial-services/fintech/fintech-insights/neobanks-and-the-next-banking-revolution.html accessed March 6, 2024

[20] Section 2(nb) of Information Technology Act 2000—cyber security‖ means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction;] "Information Technology Act 2000" (June 9, 2000) https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf accessed March 8, 2024

- Ms Valeria Ferrari, "The Platformisation of Digital Payments: The Fabrication of Consumer Interest in the EU FinTech Agenda" [2022] Journal Homepage: www.elsevier.com/locate/CLSR https://www.sciencedirect.com/science/article/pii/S0926580521003770 accessed on March 7,2024
- Jagannath J, 'RBI Imposes Penalty of Rs 3.06 Crore on Amazon Pay (India) for Violation of Norms' (*Business Today*, 3 March 2023) https://www.businesstoday.in/latest/corporate/story/rbi-imposes-penalty-of-rs-306-crore-on-amazon-pay-india-heres-why-372179-2023-03-03 accessed 8 March 2024
- Zaveri B, 'Open Questions on RBI's Enforcement Actions in Indian Fintech' (*IndiaCorpLaw*, 22 February 2024) https://indiacorplaw.in/2024/02/open-questions-on-rbis-enforcement-actions-in-indian-fintech.html accessed 8 March 2024.
- Parasher S and Mehul , 'What Happened When the RBI Cancelled Payment Aggregator Licences?' (*StartupNews.fyi*, 3 February 2024) https://startupnews.fyi/2024/02/03/what-happened-when-the-rbi-cancelled-payment-aggregator-licences/ accessed 8 March 2024.
- Xu J and Gao X, "E-Payment Systems, E-Marketing, and E-Advertising," *Intelligent information systems* (2021) https://doi.org/10.1142/9789811231841_0006 accessed on 8 March 2024
- "Securities and Exchange Board of India Regulation" https://www.sebi.gov.in/sebiweb/home/HomeAction.do?doListing=yes&sid=1&ssid=3&smid=0 accessed March 8, 2024