„Krytyka Prawa", tom 17, nr 1/2025, s. 78–96, ISSN 2080-1084, e-ISSN 2450-7938, © 2025 Authors.

ADHIP BANERJEE[1], MONA MAHECHA[2], PRANAV MATHUR[3]

Digital Payments in India: Exploring Emerging Issues in the Legal and Regulatory Framework[4]

Submitted: 8.09.2024. Accepted: 13.11.2024

Abstract

The expansion and development of the digital payment infrastructure in India's banking sector have led to a significant increase in the number and value of digital transactions. Yet, such transactions are inherently vulnerable to cybercrime, particularly digital payment fraud. According to a recent report published by the Indian Cybercrime Coordination Centre (I4C), digital financial frauds amounted to ₹1.25 lakh crore over the past three years. Data provided by the National Cybercrime Reporting Portal further indicate that in the year 2023 alone, victims of digital financial fraud incurred losses of at least ₹10,319 crore. This study aims to identify and examine the legal challenges associated with digital payments and their implications while proposing potential strategies to mitigate the existing risks. It also explores measures to enhance fund transfers and payment processes involving the use of digital means.

Keywords: financial frauds, digital payments, cybercrime, regulation, fund transfer.

[1] Adhip Banerjee – Manipal University Jaipur (India); e-mail: adhip.banerjee14@gmail.com; ORCID: 0000-0002-2277-3018.

[2] Mona Mahecha, PhD (corresponding author) – Manipal University Jaipur (India); e-mail: mona.mahecha@jaipur.manipal.edu; ORCID: 0000-0003-3900-6955.

[3] Pranav Mathur – Manipal University Jaipur (India); e-mail: pranav23102001@gmail.com; ORCID: 0009-0003-6228-2349.

[4] The research in this article has not been supported financially by any institution.

„Krytyka Prawa", tom 17, nr 1/2025, s. 78–96, ISSN 2080-1084, e-ISSN 2450-7938, © 2025 Authors.

ADHIP BANERJEE, MONA MAHECHA, PRANAV MATHUR

Płatności cyfrowe w Indiach badanie nowych problemów w ramach prawnych i regulacyjnych[5]

Streszczenie

Ekspansja i rozwój infrastruktury płatności cyfrowych w indyjskim sektorze bankowym doprowadziły do znacznego wzrostu liczby i wartości transakcji cyfrowych. Takie transakcje są jednak z natury podatne na cyberprzestępczość, w szczególności na oszustwa związane z płatnościami cyfrowymi. Według niedawnego raportu opublikowanego przez Indyjskie Centrum Koordynacji Cyberprzestępczości (I4C) cyfrowe oszustwa finansowe wyniosły 1,25 lakh crore w ciągu ostatnich trzech lat. Dane dostarczone przez National Cybercrime Reporting Portal wskazują ponadto, że tylko w 2023 r. ofiary cyfrowych oszustw finansowych poniosły straty w wysokości co najmniej 10 319 crore. Niniejszy artykuł ma na celu zidentyfikowanie i zbadanie wyzwań prawnych związanych z płatnościami cyfrowymi oraz ich konsekwencji oraz zaproponowanie potencjalnych strategii łagodzenia istniejących zagrożeń. Autorzy analizują również środki mające na celu usprawnienie transferów środków i procesów płatności z wykorzystaniem środków cyfrowych.

Słowa kluczowe: oszustwa finansowe, płatności cyfrowe, cyberprzestępczość, regulacje, przelew funduszy.

[5] Badania wykorzystane w artykule nie zostały sfinansowane przez żadną instytucję.

 DOI: 10.7206/kp.2080-1084.753

Introduction

With a considerable range of developments in the world of information technology and the advent of fin-tech institutions, there has been a global trend towards cashless payment transactions. It has been found that approximately two-thirds of adults across the globe currently use digital payments. The rate of individuals making use of digital payments in developing economies has significantly increased from 35% in 2014 to 57% in 2021. In developing economies, as of 2021, 71% of the population has an account in a bank, other financial institution, or with a mobile money provider – compared to 63% in 2017 and 42% in 2011, indicating a positive trend in financial inclusion.[6] In India, the total number of digital payment transactions increased from 20.71 billion in the financial year 2017–2018 to 134.62 billion in the financial year 2022–2023.[7] An International Monetary Fund working paper on "The Macroeconomics of De-cashing" had stated that till 2017, several countries undertook endeavours to limit cash-based transactions in order to bolster their economies.[8] It would be erroneous to observe that cashless transaction avenues opened up as a culmination of the post pandemic economic status. Rather, it was a matter of subsisting under the veil of Point of Sale (POS) by way of credit or debit cards, mobile wallets in lieu of interest and convenience fees, net banking, Electronic Clearing Service (ECS), Electronic Fund Transfer (EFT), Immediate Payment Service (IMPS), National Electronic Funds Transfer (NEFT), Real Time Gross Settlement (RTGS), and other similar mechanisms. It can be discreetly calculated that the ultimate goal of such cashless transactions is not to make denomination currency notes obsolete, but to reduce the usage of currency notes to a level that require lesser circulation of such notes in the economy and, as a corollary, to increase the value of such currency in the global market. It is necessary to consider that digital payments require some sort of redressal from at the international level in order to facilitate cross-border payment services. The G20 in 2020, with Saudi Arabia at the helm as part of its presidency, had made it a priority to simplify and enhance

---

6 World Bank Group, *COVID-19 Drives Global Surge in use of Digital Payments,* Washington, 2022. Available from: https://www.worldbank.org/en/news/press-release/2022/06/29/covid-19-drives-global-surge-in-use-of-digital-payments (accessed: 20.06.2024).

7 Ministry of Finance, *Total Digital Payment Transactions Volume Increases from 2,071 Crore in FY 2017-18 to 13,462 Crore in FY 2022-23 at a CAGR of 45 per Cent: MoS Finance*, PIB Delhi, 2023. Available from: https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1988370 (accessed: 20.06.2024).

8 A. Kireyev, *The Macroeconomics of De-Cashing*, IMF, 2017, p. 4.

cross border payments, with a common set of building blocks. Such prioritisation was addressed in a report by the Committee on Payments and Market Infrastructures (CPMI) in order to identify and enumerate such blocks where a joint collaboration of private and public sector institutions could work together in enhancing and accelerating such initiative undertaken by the G20. The foundational elements within this area include: (i) harmonising regulatory, supervisory, and oversight frameworks; (ii) ensuring the consistent and comprehensive application of AML/CFT measures; (iii) examining the interplay between data frameworks and cross-border payments; (iv) advancing the establishment of secure payment corridors; and (v) encouraging the sharing of KYC and identity information.[9]

Despite the multiple steps taken to promote digital payments and achieve the goal of arriving at a hybrid model of 'cashless economy', the corpulent hurdle in the pursuit of this goal has been financial fraud in the digital space. In 2015 and 2016, the mechanism of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) came under scrutiny as perpetrators had stolen credentials to make illegitimate transfers from Bangladesh Government's reserve account at the Federal Reserve Bank of New York that had used such network became victim of a major cyber-attack which resulted in a loss of $81 million.[10] The attack was considered as a big blow to international cashless transfers as the SWIFT system is considered as the important pillar of international money flow. After the implementation of the Government of India's demonetisation policy that had catalysed the transition from cash-based economy to cashless transactions by way of Unified Payments Interface (UPI), in August 2018, the world saw a grave attack on the Cosmos Bank in India – the oldest co-operative bank in the world's largest democracy – involving a well-planned and highly coordinated cyberattack based on malicious proxy servers sending fake responses and authorising transactions, resulting in a loss of $13.5 million, which became a bolt from the blue for India's intelligence agencies.[11] However, 11 people were convicted by the District Court of Pune in the state of Maharashtra in connection with said criminal act.[12] At around the same time,

---

9 Committee on Payments and Market Infrastructures, *Enhancing Cross-Border Payments: Building Blocks of a Global Roadmap*, Bank for International Settlements, July 2020. Available from: https://www.bis.org/cpmi/publ/d193.pdf (accessed: 20.06.2024).

10 J. Leyden, *A Typo Stopped Hackers Siphoning Nearly $1bn out of Bangladesh*, "The Register" 2016, March, Available from: https://www.theregister.com/2016/03/11/bangladesh_bank_cyber_heist_1bn_dollars_nearly_stolen/ (accessed: 20.06.2024).

11 S. Iyer, Tanksale M., Shelke G., *Cosmos Bank Hit by Cyber Hack, Loses Rs 94 Crore in 2 Days*, "The Times of India" 2018, 15 August 2018. Available from: https://timesofindia.indiatimes.com/city/pune/cosmos-bank-hit-by-cyber-hack-loses-rs-94-crore-in-2-days/articleshow/65409441.cms (accessed: 20.06.2024).

12 Press Trust of India, *11 Convicted In India's Biggest Cyberattack On Cosmos Bank* NDTV.,April 2023, Available from: https://www.ndtv.com/india-news/11-convicted-in-indias-biggest-cyberattack-on-cosmos-bank-3973428 (accessed: 20.06.2024).

 DOI: 10.7206/kp.2080-1084.753

around the same time 380,000 sets of account credentials were stolen from the British Airways website by way of phishing.[13] In light of such incidents, many states adopted several legislations and frameworks to protect consumers and facilitators from such cyberattacks and frauds, as well as bring in transparency in the digital payments landscape, promoting accountability and cross-border trust. This research paper aims to shed light on the legislative framework of digital payments and prevention of fraud in the context of Indian economy, as well as take into consideration its aims and objectives and provide suggestions of improvements that can be made to existing and proposed legislation and amendments thereto.

The legal framework governing digital payments in India

Fraud in the area of digital payments is based on a multi-factor system, including the strictness of the regulatory framework, the level of technological efficiency that is associated with it, or the legality supporting entire transactions, etc.[14] Particularly in India, the primary legislation governing all digital payment transactions is the *Payment of Settlement Systems Act, 2007* (hereinafter referred to as the "PSS Act"). It provides[15] for various rights, duties, and penalties applying to the parties involved in and overseeing the payment mechanism as a regulatory authority – namely, the Reserve Bank of India (hereinafter referred to as "the RBI"). However, it cannot be considered exhaustive or comprehensive. Various major amendments to the PSS Act have been suggested, most notably the establishment of a Payments Regulatory Board (hereinafter referred to as "PRB"), independent of the overarching control of the RBI,[16] but most of them have not even come close to being implemented.

---

13 O. Gill, O. Rudgard, *British Airways Hacked as 380,000 Sets of Payment Details Stolen*, "The Telegraph" 2018, 6 September. Available from: https://www.telegraph.co.uk/business/2018/09/06/british-airways-hacked-380000-sets-payment-details-stolen/ (accessed: 20.06.2024).

14 *Combating fraud in the era of digital payments*, I. Tomar, N. Dharukar, M. Tiwari, R. Mishra, S. Gupta, N. Surekha, M. Syamala, Pricewaterhouse Cooper, May, 2022. Available from: https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/payments-transformation/combating-fraud-in-the-era-of-digital-payments.pdf (accessed: 6.06.2024).

15 King Stubb & Kasiva, *Digital Payments in India: A Guide to Regulatory Framework*, March 2023. Available from: https://ksandk.com/banking/digital-payments-in-india-regulatory-framework/ (accessed: 6.06.2024).

16 T. Saran, A. Grover, *Payments Regulatory Board: Merits and Criticisms*, India Corp Law, October 2018. Available from: https://indiacorplaw.in/2018/10/payments-regulatory-board-merits-criticisms.html (accessed: 6.06.2024).

An independent Payments Regulatory Board

Under the current regime of the PSS Act,[17] the RBI has the power to establish a PRB for the purposes of regulating digital payments, known as the *Board for Regulation and Supervision of Payment and Settlement Systems* (hereinafter referred to as "the BPSS"), the main duties[18] of which include the regulation, establishment of standards and policies, etc. for all digital payments in India.

However, the point of contention began when an *Inter-Ministerial Committee for Finalisation of Amendments of the PSS Act, 2007* was formed under the aegis of the Ministry of Finance, which submitted its final report[19] in 2018. The report suggested the establishment of an independent PRB among other amendments to the PSS Act, thereby diluting the regulatory hold of the RBI over the realm of digital payments in India. Among other benefits, it included the positions of a full-time director and four full-time members, in order to achieve a broader representation in the Board itself.

In response, the RBI itself issued a dissent note,[20] disagreeing with the recommendations that were so put forward. In particular, it stated that payments, in general, are considered a subset of currency itself, which is directly under the control of RBI. Further, the RBI declared that there had not been any problems with the payment systems in India, which guaranteed no shift or departure from the current regime. It also placed emphasis on the then-current composition of the Board, and that it was efficient in its functioning. However, a look at RBI's annual report[21] of 2021–2022 reveals that card and internet fraud that had been reported saw a 34% increase from the previous financial year, and these numbers and percentages have always been on an upwards trajectory since then.

---

17 The Payments and Settlement Systems Act, 2007, S. 3(2), No. 51, Acts of Parliament, 2007 (India).

18 Reserve Bank Of India, *Payment and Settlement Systems*. Available from: https://www.rbi.org.in/scripts/FS_Overview.aspx?fn=9#:~:text=The%20Board%20for%20Regulation%20and,on%20payment%20systems%20in%20RBI (accessed: 6.06.2024).

19 Department of Economic Affairs, *Report of the Inter-Ministerial Committee for Finalisation of Amendments to the PSS Act, 2007*, Ministry of Finance, August 2018. Available from: https://dea.gov.in/sites/default/files/Payment%20and%20settlement.pdf (accessed: 6.06.2024).

20 Reserve Bank Of India, *Reserve Bank of India releases Dissent Note on Inter-Ministerial Committee for Finalization of Amendments to PSS Act*, Department of Communication, October 2018. Available from: https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR929D2386330293E4E6A8E8E2CC5C28D2C05.PDF (accessed: 6.06.2024).

21 Reserve Bank Of India, *Payment and Settlement Systems and Information Technology*, 2022. Available from: https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/9PAYMENTANDSETTLEMENT033C9414C22C4370AD16C837C55EDDC9.PDF (accessed: 6.06.2024).

 DOI: 10.7206/kp.2080-1084.753

There exist various examples, particularly the United Kingdom as well as Australia,[22] where functions of a regulatory agency are not the sole prerogative of the central bank; rather, they rest concurrently with multiple entities, serving as a testament to counter one of the most prominent claims made by the RBI in its dissent note. Therefore, the dissent shown by the RBI stands on a shaky foundation. The Mission statement of RBI in the Vision document of 2009–2012 with regards to whether the payment and settlement systems have been made more fast, secure, accessible, safe and authorised[23] is still not achived.

Apart from an independent PRB, the RBI should take cognizance of its vast jurisdiction and numerous roles that it plays, and consider that since it itself acts as a service provider, its role as an entity which settles disputes between other service providers or participants may be viewed as questionable.

The shift from paper to electronic

According to the PSS Act, even though a payment system can only be established by the authorisation of the RBI,[24] which limits the quantity of operative payment systems, a vast majority of Indians use digital interfaces for payment, such as the Bharat Interface for Money (hereinafter referred to as "BHIM"), or the Unified Payments Interface (hereinafter referred to as "UPI"). The value of transactions made through UPI has doubled in the last two years, with a current monetary value of over ₹20 lakh crore.[25] Almost all other similar payment systems show an upwards trajectory as well. However, simultaneously, the value of Currency in Circulation (hereinafter referred to as "CiC") has also grown by an exponential amount, with its ratio to the Gross Domestic Product peaking at 14.4% during 2021–2022.[26] Both these positive trends posed to be a counterintuitive paradox, given that the forms of digital payment were viewed as being a substitute to CiC itself.[27] However, it

---

22 The Australian Government the Treasury data, *Payments System Modernisation: Regulation of payment service providers*, December 2023. Available from: https://treasury.gov.au/sites/default/files/2023-12/c2023-469663-cp.pdf (accessed: 6.06.2024).

23 Reserve Bank Of India, *Payment Systems in India – Vision 2009-12*. Available from: https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/VIS01092009.pdf (accessed: 6.06.2024).

24 The Payments and Settlement Systems Act, 2007, S. 4, No. 51, Acts of Parliament, 2007 (India).

25 National Payments Corporation of India, *UPI Product Statistics*. Available from: https://www.npci.org.in/what-we-do/upi/product-statistics (accessed: 6.06.2024).

26 Reserve Bank Of India, *Currency Management*, 2022. Available from: https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/8CURRENCYMANAGEMENT8AC7498F4E694954ACB94098D70BB626.PDF (accessed: 6.06.2024).

27 Reserve Bank Of India, *Annual Report 2022-23,* 2023. Available from: https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/0ANNUALREPORT20222322A548270D6140D998AA20E8207075E4.PDF (accessed: 6.06.2024).

must be taken into account that a lot of currency is kept for unpredictable emergency circumstances, the most recent example of which is the COVID pandemic, which justifies the existence of the paradox.

Despite this information, one of the most common legal and regulatory roadblocks that has persisted is the promotion and growth of Digital Financial Literacy (hereinafter referred to as "DFL"). Even though some opinions have credited the COVID pandemic for accelerating DFL[28] among Indians, with record growth among rural sectors and making up 36% of all digital transactions in the previous years,[29] the RBI still considers the penetration of digitalisation a common challenge in its publication titled *Payment and Settlement Systems in India – Journey in the Second Decade of the Millenium*.[30] DFL has largely remained a concern pertaining to the regulatory framework. Its integration in legislations would serve to be an effective method of promotion. For instance, if a legislation mandates the filing of any application, or some document on an online portal, with appropriate accompanying frameworks, it would increase the penetration of digital literacy by a few percentage points.

Grievance redressal in case of fraud in India

The statistics reflecting the rate of digital payments fraud in the country, as presented hereinabove, are nothing short of concerning. The PSS Act will have to be amended in order to comprehensively address fraudulent transactions and work in conjunction with the Information Technology Act of 2000 (hereinafter referred to as the "IT Act") to successfully tackle the practice.

One of the main amendments discussed is the introduction of payment service providers into the realm of consumer protection.[31] Various inaccuracies in the system, or the fact that the system is prone to a compromise in data protection, etc. are not

---

28 S. Chaddha, S. Jain, *Digital Transformation of Financial Sector in India – Evolution, Issues and Challenges*, MCR HRD Institute, January 2024. Available from: https://www.mcrhrdi.gov.in/images/samriddhi/number2/10.Digital%20Transformation%20of%20Financial%20Sector%20in%20India.pdf (accessed: 6.06.2024).

29 TransUnion CIBIL with data insights from NPCI and FCC, *The Rise and Evolution of India's Digital Finance*, The Global Fintech Fest, 2023. Available from: https://www.npci.org.in/PDF/npci/knowledge-center/partner-whitepapers/The-Rise-and-Evolution-of-India's-Digital-Finance.pdf (accessed: 6.06.2024).

30 Reserve Bank Of India, *Payment and Settlement Systems in India: Journey in the Second Decade of the Millennium*. 2021. Available from: https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/PSSBOOKLET93D3AEFDEAF14044BC1BB36662C41A8C.PDF (accessed: 6.06.2024).

31 S. Ahmed, A. Babele, *Modernising the Law for Payment Services in India | Preparing for the Future of Retail Payments*, Vidhi Legal Policy, September 2021. Available from: https://vidhilegalpolicy.in/wp-content/uploads/2021/10/Modernising-the-law-for-Payment-Services-in-India-Preparing-for-the-Future-of-Retail-Payments.pdf (accessed: 14.06.2024).

 DOI: 10.7206/kp.2080-1084.753

due to the inefficiency of payment service providers, but due to an inefficiently designed or approved system *ab initio.* Even though the RBI releases circulars and notifications for these from time to time, the frequency and amount of such inconsistencies demands their integration with primary legislation. Not only is this beneficial for payment service providers, but all of the entities also involved in a digital transaction benefit from a positive image in the public finance realm.

It has been observed that the nature, forms, and methods of fraud have evolved over time. Other than actively investing in consumer awareness, the PSS Act and the IT Act must impose stricter punishments on individuals or organisations guilty of fraudulent activities targeting payment systems, having a separate fraud management solution[32] network in place, governed by these acts and complementary notifications and regulations identifying fraud channels and punishing them robustly.

The advent of artificial intelligence[33] and machine learning systems in the detection of fraud has saved the global economy millions of dollars. Moreover, it is evolving daily, with systems now able to consume historical data and figures in order to predict fraud and be equipped with preventive measures.[34] Fostering such kind of research and development in order to come up with indigenous intelligence systems is a policy initiative in the hands of legislators.

The RBI, exercising its powers under the mandate of the PSS Act,[35] initiated the *Ombudsman Scheme for Digital Transactions,*[36] *2019* (hereinafter referred to as "the OSDT"), an office created to take measures regarding grievance redressal in cases of digital payments made by consumers. Even though it has been integrated into the RBI – Integrated Ombudsman Scheme,[37] 2021, neither of the Schemes refer to *fraud* and its various sub-types as a separate and explicit ground for filing a complaint. The content of the Scheme must be changed in order to include fraud in its

---

32 K. Sarkar, T. Bhatt, K. Mahajan, A. Budhiraja, D. Duttagupta, S. Patel, *The Indian payments handbook – 2023–2028*, Pricewaterhouse Cooper, 2023. Available from: https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/publications/the-indian-payments-handbook-%E2%80%93-2023%E2%80%932028.pdf (accessed: 14.06.2024).

33 INFOSYS BPM, *AI in the banking sector: How fraud detection with AI is making banking safer.* Available from: https://www.infosysbpm.com/blogs/bpm-analytics/fraud-detection-with-ai-in-banking-sector.html (accessed: 14.06.2024).

34 N.F. Ryman-Tubb, P.L. Krause, W. Garn, *How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark*, "Engineering Applications of Artificial Intelligence" 2018, pp. 130–136. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0952197618301520?via%3Dihub (accessed: 14.06.2024).

35 The Payments and Settlement Systems Act, 2007, S. 18, No. 51, Acts of Parliament, 2007 (India).

36 Reserve Bank Of India, *Ombudsman Scheme for Digital Transactions, 2019.* Available from: https://rbidocs.rbi.org.in/rdocs/Content/PDFs/OSDT31012019.pdf (accessed: 6.06.2024).

37 Reserve Bank Of India, *The Reserve Bank – Integrated Ombudsman Scheme, 2021*, November 2021. Available from: https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR1184E54DDADDA7BF415F957FE12C19A06055.PDF (accessed: 6.06.2024).

domain directly, and secondary legislation may be made in order to supplement such inclusion.

An overview of legislative framework in the European Union

Within the European Union, every state reserves the right to preserve their sovereignty and, at the same time, frame their own independent legislations. However, most of such legislation is influenced by the framework laid down by the European Union, which is non-binding in nature and thereby giving each state space to bend and mend such laws to fit their own needs and challenges. Electronic payments in the European Union are regulated by the backbone of all the regulations – that is the Single Euro Payments Area (SEPA), where the market is consolidated for the purpose of electronic transactions for both consumers and businesses. However, the implementation of SEPA has encountered various challenges in achieving homogeneity due to various domestic laws adopted earlier by the European states.[38] To bring all states together on the same playing field, the European Commission had issued a non-binding recommendation that was applicable to all digital transactions from every part of the world by way of money instruments, including deposit and withdrawal.[39] It required minimum information and outlined the rights and obligations of both the issuer and the recipient for protection against digital frauds. This set of regulations as per the relevant directives was only adopted by Belgium as part of its national legal system, but in 2007, such directives were in dire need of revision as they were overlapping and contradictory in nature.[40]

Financial losses suffered by banks as a result of digital fraud are accounted for using the operational risk capital standard. As per the revised Basel III operational risk framework,[41] a bank's operational risk Pillar 1 capital requirements are calculated by multiplying its business indicator component (a measure of business volume) by the internal loss multiplier. This multiplier represents the bank's average historical operational risk losses over the past ten years. There are seven categories of losses that are identified, including external fraud and internal fraud, which are

38 S. Mercado-Kierkegaard, *Harmonising the Regulatory Regime for Cross-Border Payment Services*, "Computer Law & Security Review" 2007, 23(2), pp. 177–187. Available from: https://doi.org/10.1016/j.clsr.2006.11.003 (accessed: 14.06.2024).

39 T. Christiansen, *Tensions of European Governance: Politicized Bureaucracy and Multiple Accountability in the European Commission*, "Journal of European Public Policy" 1997, 4(1), pp. 73–90.

40 Reserve Bank Of India, *Integrated Ombudsman…, op. cit.*

41 Basel Framework, https://www.bis.org/basel_framework/index.htm (accessed: 20.06.2024).

usually relevant to digital fraud. Consequently, Pillar 1 capital requirements for operational risk should, in principle, encompass losses resulting from digital fraud. In practice, this depends on two factors:[42]

> "(i) Whether banks are responsible for reimbursing customers for losses from digital fraud, potentially putting the banks at risk of financial losses.
> (ii) Whether supervisors have opted to include banks' historical losses in the calculation of operational risk capital requirements, rather than exercising the national discretion to set the internal loss multiplier at one, which would exclude historical losses."

When calculating their regulatory capital charge for operational risk using internal models, banks under Basel II took into account losses from digital fraud if they were using the Advanced Measurement Approach (AMA). Some jurisdictions, like Canada and Japan, have factored in digital fraud into banks' AMA operational risk calculations. Although the AMA is no longer available under the revised Basel III framework, there have been significant expansions in the requirements for loss data collection. Now, even larger banks are required to document internal losses and publicly share their annual loss data, regardless of any previous flexibility granted to them by national regulations.[43]

As part of the Pillar 2 supervisory review process, it is expected that banks maintain sufficient capital to mitigate all the risks associated with their operations. Additionally, banks are encouraged to adopt and implement advanced risk management mechanisms to effectively monitor and manage these risks.

It is important to address the risks associated with digital fraud, such as financial losses and reputational risks, under Pillar 2 if they are significant and not adequately covered by Pillar 1 capital requirements. All material risks faced by banks should be included in the bank's Internal Capital Assessment Process (ICAAP). This process ensures that the bank has enough capital to address its risks, going beyond the minimum requirements.[44] However, it is important to note that solely increasing capital may not be the most effective method for mitigating risks. Additional measures that should be considered include strengthening risk management,

---

42 E.I. Altman, G. Sabato, *Effects of the New Basel Capital Accord on Bank Capital Requirements for SMEs*, "Journal of Financial Services Research" 2005, pp. 15–42. Available from: http://link.springer.com/10.1007/s10693-005-4355-5 (accessed: 22.06.2024).

43 J. Young, *Preparedness of Banks to Be Compliant with the Criteria for the Advanced Measurement Approach: A South African Perspective*, "Corporate Ownership & Control" 2011, 8(2), pp. 44–53.

44 M.V. Goncharova, *Basel II International Convention: Four Principles of Supervisory Review Process*, "Science Journal of VolSU. Jurisprudence" 2016, 15(4), p. 155.

implementing internal limits, enhancing provisions and reserves, and improving internal controls. Furthermore, experts assess the efficacy of banks' risk management practices and implement appropriate actions when necessary.[45]

Liability of payment service providers

The Payment Services Directive (PSD) specifies the distribution of responsibility in cases of unauthorized payment transactions. According to Article 54.1 of the directive, a payment transaction is considered authorised only if the payer has given consent for it to be carried out. If consent is not given, the transaction is deemed unauthorised. Article 54.4 stipulates that the payer and the payment service provider must mutually agree on the method for transmitting consent. Furthermore, according to Article 42.2, it is required that the process and method of obtaining consent be included in the contractual terms and communicated to the payment service user (i.e. the client or payer) well before they are obligated to fulfil their contract. Article 41.1 mandates that these conditions must be communicated in a clear and comprehensible manner and made available in a lasting format for future consultation.

An essential provision for assigning responsibility in unauthorised transactions is the differentiation between transactions that take place prior to and subsequent to the notification of loss, theft, or misuse of the payment instrument. Articles 56 and 57 of the directive impose substantial notification requirements on both the payment service provider (such as the bank that issued the electronic payment instrument) and the payment service user.

When a payment instrument is reported lost, stolen, or misappropriated, the payment service provider takes responsibility for any financial consequences that may arise from subsequent transactions. Article 61.4 relieves the payment service user of any liability after receiving such notification, as long as there was no fraudulent behaviour on their part. The provider's ability to prevent further use of the instrument after notification is not significant. In addition, Article 57 mandates that the payment service provider must always have mechanisms in place to notify users of any loss, theft, or misappropriation, ensuring that users can report any issues at any time, even on weekends.

If the payment service provider fails to fulfil this obligation, they will be held responsible for all transactions that took place prior to the user's attempt to notify them and until the actual notification is made. On the other hand, the payment

[45] *Idem*, *Basel II International Convention: The Content and Targets of Supervisory Review Process*, "Legal Concept" 2017, 16(1).

 DOI: 10.7206/kp.2080-1084.753

service user bears the responsibility for any losses resulting from the use of a lost or stolen payment instrument, or if they neglected to protect the personalized security features, until they notify the appropriate parties. The liability is limited to €150, unless the user engaged in fraudulent or grossly negligent behavior, in which case Article 61.2 holds the user completely accountable.

Review and Conclusions

Ensuring the protection and security of digital identities for both consumers and businesses is of utmost importance in the field of omnichannel fraud and risk management services in the upcoming decade. At the same time, there is a continued demand among consumers for strong online and mobile channels that cater to a wide range of activities, including enrolment, payments, banking transactions, and consumer protection in the digital economy. It is necessary for banks, payment service providers, and payment processors to provide a smooth customer service experience on different platforms, such as cards, cardless transactions, omnichannel services, and open banking.

- **Establishment of an Independent Payments Regulatory Board (PRB)**
  Under the current framework of the Payment and Settlement Systems Act, 2007 (PSS Act), the Reserve Bank of India (RBI) has the authority to appoint the Board for Regulation and Supervision of Payment and Settlement Systems (BPSS). Despite its mandate, the efficiency and objectivity of the BPSS have come into question, particularly due to the RBI's dual role as a regulator and service provider. The 2018 report by the Inter-Ministerial Committee recommended forming an independent Payments Regulatory Board (PRB) to ensure broader representation and dilute RBI's overarching control.
  - **Suggestions:**
    1. Legislation for an independent PRB: Amend the PSS Act to establish an independent PRB, separate from the RBI. This board should include representatives from various sectors, including consumer rights groups, technology experts, and financial institutions.
    2. Enhanced oversight and accountability: The PRB should be required to publish regular reports on the state of digital payments, including fraud statistics, system efficiency, and consumer satisfaction. This transparency would foster greater accountability and trust in the digital payments infrastructure.

3. International models: Draw from international models like the UK's Financial Conduct Authority (FCA) and Australia's Payments System Board, which operate independently of their central banks, ensuring a balanced and efficient regulatory environment.

- **Promotion of Digital Financial Literacy (DFL)**
  Despite significant growth in digital transactions, the widespread adoption of Digital Financial Literacy (DFL) remains a challenge. The COVID-19 pandemic accelerated DFL, especially in rural areas, yet the RBI's reports indicate persistent challenges in this domain.
  - **Suggestions:**
    1. Mandate DFL programmes: Amend the PSS Act to require financial institutions to conduct regular DFL programmes, especially targeting underserved and rural populations. These programmes should cover basic digital payment methods, cybersecurity practices, and fraud prevention.
    2. Integration with education systems: Collaborate with educational institutions to integrate DFL into school and college curriculums. This would ensure that future generations are well-versed in digital payment systems from a young age.
    3. Use of technology: Leverage technology, such as mobile applications and interactive platforms, to deliver DFL content in regional languages, making it accessible to a wider audience.

- **Grievance redressal and fraud management**
  The increasingly numerous instances of digital payment fraud necessitate robust mechanisms for grievance redressal and fraud management. The current Ombudsman Scheme for Digital Transactions (OSDT) and its successor, the RBI-Integrated Ombudsman Scheme, do not explicitly address fraud as a separate ground for complaints.
  - **Suggestions**:
    1. Explicit inclusion of fraud in legislation: Amend the PSS Act and the IT Act to explicitly address various types of digital payment fraud. Establish a dedicated fraud management unit within the PRB to handle such cases.
    2. Stricter penalties and fraud management solutions: Introduce stricter penalties for individuals and organisations involved in fraudulent activities. Implement advanced fraud detection systems using artificial intelligence and machine learning to predict and prevent fraud.

 DOI: 10.7206/kp.2080-1084.753

3. Consumer protection measures: Mandate payment service providers to refund unauthorised transactions promptly and ensure robust mechanisms for reporting and resolving fraud complaints.

- **Adopting best practices from the European Union**

  The European Union's regulatory framework, particularly the Single Euro Payments Area (SEPA), provides a cohesive model for electronic transactions. The Payment Services Directive (PSD) outlines clear provisions for consumer protection and liability in cases of unauthorised transactions.

  - **Suggestions:**
    1. Adopt a SEPA-like framework: Implement a uniform framework similar to SEPA to standardise digital payment processes across India. This would simplify cross-border transactions and enhance the efficiency of digital payments.
    2. Consumer liability protection: Incorporate provisions from the PSD into Indian legislation, ensuring that consumers are protected from unauthorised transactions and that service providers are held accountable for security breaches.
    3. Operational risk management: Align with the Basel III operational risk framework to ensure that banks and payment service providers account for digital fraud in their risk management strategies. This includes maintaining adequate capital reserves and implementing robust internal controls.

- **Enhancing regulatory and supervisory framework**

  The dual role of the RBI as both regulator and service provider creates potential conflicts of interest. An independent supervisory mechanism would enhance the objectivity and efficiency of digital payment regulations.

  - **Suggestions:**
    1. Separate regulatory and service functions: Clearly define the roles of the RBI and the proposed PRB, ensuring that the RBI focuses on monetary policy while the PRB regulates digital payments.
    2. Regular audits and reviews: Mandate regular audits and reviews of digital payment systems by independent agencies. This would ensure compliance with regulatory standards and identify areas for improvement.
    3. Stakeholder engagement: Establish forums for regular interaction between regulators, service providers, and consumers. This would facilitate the exchange of feedback and foster collaborative efforts to enhance the digital payments infrastructure.

The scale and evolving nature of card fraud losses highlight the critical need for the implementation of comprehensive security measures, reinforced by appropriate fraud and risk prevention solutions. A single fraud prevention mechanism is inadequate for effectively combating fraud; each solution has its own strengths and limitations. A layered approach, employing multiple tools, can address various types of fraud, although this approach carries the risk of false rejections due to reliance on numerous tools.

Identifying the most advantageous assortment of tools to address the matter is a complex task, considering limitations such as a company's financial resources, workforce availability, and their expertise and proficiency levels. Outsourcing technology and fraud expertise is a feasible solution to overcome the constraints of rigid legacy systems. Moreover, it is crucial to incorporate state-of-the-art fraud prevention tools alongside comprehensive fraud and risk prevention services that can effectively handle automatic customer onboarding, digital identities, dispute resolution, fraud cases, and cross-border fraud data throughout India nd beyond.

References

Ahmed S., Babele A., *Modernising the Law for Payment Services in India | Preparing for the Future of Retail Payments*, Vidhi Legal Policy, September 2021. Available from: https://vidhilegalpolicy.in/wp-content/uploads/2021/10/Modernising-the-law-for-Payment-Services-in-India-Preparing-for-the-Future-of-Retail-Payments.pdf (accessed: 14.06.2024).

Altman E.I., Sabato G., *Effects of the New Basel Capital Accord on Bank Capital Requirements for SMEs*, "Journal of Financial Services Research" 2005, pp. 15–42. Available from: http://link.springer.com/10.1007/s10693-005-4355-5 (accessed: 22.06.2024).

Basel Framework, https://www.bis.org/basel_framework/index.htm (accessed: 20.06.2024).

Chaddha S., Jain S., *Digital Transformation of Financial Sector in India – Evolution, Issues and Challenges*, MCR HRD Institute, January 2024. Available from: https://www.mcrhrdi.gov.in/images/samriddhi/number2/10.Digital%20Transformation%20of%20Financial%20Sector%20in%20India.pdf (accessed: 6.06.2024).

Christiansen T., *Tensions of European Governance: Politicized Bureaucracy and Multiple Accountability in the European Commission*, "Journal of European Public Policy" 1997, 4(1), pp. 73–90. doi.org/10.1080/135017697344244.

Committee on Payments and Market Infrastructures, *Enhancing Cross-Border Payments: Building Blocks of a Global Roadmap*, Bank for International Settlements, July 2020. Available from: https://www.bis.org/cpmi/publ/d193.pdf (accessed: 20.06.2024).

Department of Economic Affairs, *Report of the Inter-Ministerial Committee for Finalisation of Amendments to the PSS Act, 2007*, Ministry of Finance, August 2018. Available from: https://dea.gov.in/sites/default/files/Payment%20and%20settlement.pdf (accessed: 6.06.2024).

Gill O., Rudgard O., *British Airways Hacked as 380,000 Sets of Payment Details Stolen*, "The Telegraph" 2018, 6 September. Available from: https://www.telegraph.co.uk/business/2018/09/06/british-airways-hacked-380000-sets-payment-details-stolen/ (accessed: 20.06.2024).

Goncharova M.V., *Basel II International Convention: Four Principles of Supervisory Review Process*, "Science Journal of VolSU. Jurisprudence" 2016, 15(4). doi: 10.15688/jvolsu5.2016.4.24.

Goncharova M.V., *Basel II International Convention: The Content and Targets of Supervisory Review Process*, "Legal Concept" 2017, 16(1). doi: 10.15688/lc.jvolsu.2017.1.25.

INFOSYS BPM, *AI in the banking sector: How fraud detection with AI is making banking safer*, Avaiable from: https://www.infosysbpm.com/blogs/bpm-analytics/fraud-detection-with-ai-in-banking-sector.html (accessed: 14.06.2024).

Iyer S., Tanksale M., Shelke G., *Cosmos Bank Hit by Cyber Hack, Loses Rs 94 Crore in 2 Days*, "The Times of India" 2018, 15 August 2018. Available from: https://timesofindia.indiatimes.com/city/pune/cosmos-bank-hit-by-cyber-hack-loses-rs-94-crore-in-2-days/articleshow/65409441.cms (accessed: 20.06.2024).

King Stubb & Kasiva, *Digital Payments in India: A Guide to Regulatory Framework*, March 2023. Available from: https://ksandk.com/banking/digital-payments-in-india-regulatory-framework/ (accessed: 6.06.2024).

Kireyev A., *The Macroeconomics of De-Cashing*, IM 2017. doi: 10.5089/9781475589252.001.

Leyden J., *A Typo Stopped Hackers Siphoning Nearly $1bn out of Bangladesh*, "The Register" 2016, March. Available from: https://www.theregister.com/2016/03/11/bangladesh_bank_cyber_heist_1bn_dollars_nearly_stolen/ (accessed: 20.06.2024).

Mercado-Kierkegaard S., *Harmonising the Regulatory Regime for Cross-Border Payment Services*, "Computer Law & Security Review" 2007, 23(2), pp. 177–187. Available from: https://doi.org/10.1016/j.clsr.2006.11.003 (accessed: 14.06.2024).

Ministry of Finance, *Total Digital Payment Transactions Volume Increases from 2,071 Crore in FY 2017-18 to 13,462 Crore in FY 2022-23 at a CAGR of 45 per Cent: MoS Finance*, PIB Delhi, 2023. Available from: https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1988370 (accessed: 20.06.2024).

National Payments Corporation of India, *UPI Product Statistics*. Available from: https://www.npci.org.in/what-we-do/upi/product-statistics (accessed: 6.06.2024).

Press Trust of India, *11 Convicted In India's Biggest Cyberattack On Cosmos Bank* NDTV.,April 2023, Available from: https://www.ndtv.com/india-news/11-convicted-in-indias-biggest-cyberattack-on-cosmos-bank-3973428 (accessed: 20.06.2024).

Reserve Bank Of India, *Annual Report 2022-23,* 2023. Available from: https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/0ANNUALREPORT20222322A548270D6140D998AA20E8207075E4.PDF (accessed: 6.06.2024).

Reserve Bank Of India, *Currency Management*, 2022. Available from: https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/8CURRENCYMANAGEMENT8AC7498F4E694954ACB94098D70BB626.PDF (accessed: 6.06.2024).

Reserve Bank Of India, *Ombudsman Scheme for Digital Transactions, 2019*. Available from: https://rbidocs.rbi.org.in/rdocs/Content/PDFs/OSDT31012019.pdf (accessed: 6.06.2024).

Reserve Bank Of India, *Payment and Settlement Systems and Information Technology*, 2022. Available from: https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/9PAYMENTANDSETTLEMENT033C9414C22C4370AD16C837C55EDDC9.PDF (accessed: 6.06.2024).

Reserve Bank Of India, *Payment and Settlement Systems in India: Journey in the Second Decade of the Millennium*. 2021. Available from: https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/PSSBOOKLET93D3AEFDEAF14044BC1BB36662C41A8C.PDF (accessed: 6.06.2024).

Reserve Bank Of India, *Payment and Settlement Systems*. Available from: https://www.rbi.org.in/scripts/FS_Overview.aspx?fn=9#:~:text=The%20Board%20for%20Regulation%20and,on%20payment%20systems%20in%20RBI (accessed: 6.06.2024).

Reserve Bank Of India, *Payment Systems in India – Vision 2009-12*. Available from: https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/VIS01092009.pdf (accessed: 6.06.2024).

Reserve Bank Of India, *Reserve Bank of India releases Dissent Note on Inter-Ministerial Committee for Finalization of Amendments to PSS Act*, Department of Communication, October 2018. Available from: https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR929D2386330293E4E6A8E8E2CC5C28D2C05.PDF (accessed: 6.06.2024).

Reserve Bank Of India, *The Reserve Bank – Integrated Ombudsman Scheme, 2021*, November 2021. Available from: https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR1184E54DDADDA7BF415F957FE12C19A06055.PDF (accessed: 6.06.2024).

Ryman-Tubb N.F., Krause P.L, Garn W., *How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark*, "Engineering Applications of Artificial Intelligence" 2018, pp. 130–136. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0952197618301520?via%3Dihub. (accessed: 14.06.2024).

Saran T., Grover A., *Payments Regulatory Board: Merits and Criticisms*, India Corp Law, October 2018. Available from: https://indiacorplaw.in/2018/10/payments-regulatory-board-merits-criticisms.html (accessed: 6.06.2024).

Sarkar K., Bhatt T., Mahajan K., Budhiraja A., Duttagupta D., Patel S., *The Indian payments handbook – 2023–2028*, Pricewaterhouse Cooper, 2023. Available from: https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/publications/the-indian-payments-handbook-%E2%80%93-2023%E2%80%932028.pdf (accessed: 14.06.2024).

The Australian Government the Treasury data, *Payments System Modernisation: Regulation of payment service providers*, December 2023. Available from: https://treasury.gov.au/sites/default/files/2023-12/c2023-469663-cp.pdf (accessed: 6.06.2024).

The Payments and Settlement Systems Act, 2007, S. 18, No. 51, Acts of Parliament, 2007 (India).

The Payments and Settlement Systems Act, 2007, S. 3(2), No. 51, Acts of Parliament, 2007 (India).

The Payments and Settlement Systems Act, 2007, S. 4, No. 51, Acts of Parliament, 2007 (India).

Tomar I., Dharukar N., Tiwari M., Mishra R., Gupta S., Surekha N., Syamala M., *Combating fraud in the era of digital payments*, Pricewaterhouse Cooper, May, 2022, Available

from: https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/payments-transformation/combating-fraud-in-the-era-of-digital-payments.pdf (accessed: 6.06.2024).

TransUnion CIBIL with data insights from NPCI and FCC, *The Rise and Evolution of India's Digital Finance*, The Global Fintech Fest, 2023. Available from: https://www.npci.org.in/PDF/npci/knowledge-center/partner-whitepapers/The-Rise-and-Evolution-of-India's-Digital-Finance.pdf (accessed: 6.06.2024).

World Bank Group, *COVID-19 Drives Global Surge in use of Digital Payments,* Washington, 2022. Available from: https://www.worldbank.org/en/news/press-release/2022/06/29/covid-19-drives-global-surge-in-use-of-digital-payments (accessed: 20.06.2024).

Young J., *Preparedness of Banks to Be Compliant with the Criteria for the Advanced Measurement Approach: A South African Perspective*, "Corporate Ownership & Control" 2011, 8(2), pp. 44–53. doi: 10.22495/cocv8i2sip4.