FINTECH CONTRACTS IN INDIA: USING CYBERSECURITY CLAUSES FOR CONSUMER SAFETY

Srijopriyo Das, B.A.LL.B., Symbiosis Law School, Hyderabad, Symbiosis International (Deemed) University, Pune.

Arkya Banerjee, BA. LLB, Symbiosis Law School, Hyderabad, Symbiosis International (Deemed) University, Pune.

ABSTRACT

While digital payment innovation in India has improved transaction efficiency, it has also created novel vulnerabilities for consumers due to fraud and infrastructure issues. The purpose of this paper is to recast digital payment security as a central theme within the framework of consumer protection law because insecure digital payments systems amount to inferior digital service provision under the Consumer Protection Act, 2019. Nevertheless, conventional consumer law remains inherently reactive and ineffective at addressing the speed, complexity, and shared liabilities of digital financial malpractice.

It will be argued that consumer protection law is becoming more contractualised in the Indian digital payments space where cybersecurity provisions, indemnities, audits, and liability distribution measures have been entrenched in private law through fintech contracts, constituting a covert form of private governance of digital finance. Despite its effectiveness in overcoming regulatory deficiencies, there are concerns of privity, opacity, algorithms, unconscionability, and insolvency of fintech firms underpinning such contractualization.

Comparative law perspectives from the UK, EU, and Brazil will be considered to highlight the need for active regulation of such private forms of governance of digital finance.

Keywords: Digital Consumer Protection, Fintech Regulation, Contractual Governance, Digital Payment Security, Cyber Risk Allocation.

1. INTRODUCTION

There has been a revolution in India in digital payment in which consumers transact with platforms such as ***Unified Payments Interface (UPI)*****,** digital wallets, and embedded fintechs. This is no longer the case with the scale and success of this transition overtaking early scepticism regarding infrastructural limitations and financial inclusion that was once brought up in parliamentary debates[1].

Even though accessibility and efficiency have improved due to the rapid financial digitalisation, there exists consumer vulnerability. Sending out fraudulent payment requests, phishing, impersonation scams, backend data breaches, and authentication failures not only put consumers in financial danger because of negligence but also due to the systemic vulnerabilities within digital payment infrastructures[2].

Unfortunately, consumer law remains largely inactive in such cases and only offers remedies after harm has been caused. Besides, the digital payment ecosystem remains inadequately addressed even after fragmented frameworks under the ***Consumer Protection Act, 2019[3], Payment and Settlement Systems Act, 2007[4]***, and the ***Digital Personal Data Protection Act, 2023[5].*** Modern payment transactions operate on various banks, aggregators, gateways, processors, and third-party vendors, thus making the financial security of the consumer reliant on the backend contractual arrangements rather than direct statutory safeguards[6].

The essay argues that the consumer protection in India's digital payments sector is contractually deeper. The growing inclusion of cybersecurity obligations, indemnity clauses, audit rights and liability-allocation measures in the fintech contracts serves as an invisible layer of private consumer protection[7]. Such contracts fill the gap in regulation but also raise industrial issues, including privity, ambiguity, automated decision-making, and low bargaining capacity[8]. The question remains as to whether this provides for a stronger consumer safety or just shifts

[1] India Lok Sabha Debates, Budget Session 2017–18 (statement of P. Chidambaram).
[2] Reserve Bank of India, *Report on Trend and Progress of Banking in India 2022–23* (2023); Indian Computer Emergency Response Team (CERT-In), *Annual Report 2023*.
[3] Consumer Protection Act, 2019, No. 35 of 2019, INDIA CODE.
[4] Payment and Settlement Systems Act, 2007, No. 51 of 2007, INDIA CODE.
[5] Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE.
[6] National Payments Corporation of India (NPCI), *UPI Product Statistics* (2024); NASSCOM, *Cybersecurity in Digital Payments Ecosystem* (2023).
[7] OECD, *Digital Security Risk Management for Economic and Social Prosperity* (2019); NASSCOM, *Model Technology Contract Clauses* (2024).
[8] *Central Inland Water Transport Corp. v. Brojo Nath Ganguly,* (1986) 3 SCC 156 (India).

the consumer risk.

2. DIGITAL PAYMENTS AS A SPHERE OF CONSUMER PROTECTION

2.1 Reconceptualising Payment Security as Consumer Safety

The rise of the digital payment system in India has changed the payment infrastructure into a direct location of consumer susceptibility. Historically, the focus of consumer protection law was on flawed physical products and subpar offline services, but within the digital economy, the insecure digital systems can cause equally serious damage[9]. In the area where consumers use UPI systems, payment gateways, banking applications, and fintech interfaces to conduct their daily transactions, the safety and integrity of the system is a part of the security of the service being used[10]. Therefore, the security of digital payments should be considered as a consumer protection, and not just a financial regulation issue.

The ***Consumer Protection Act*** broadly defines "*service*" in ***Section 2(42)*** and identifies "*deficiency*" in ***Section 2(11)*** as encompassing inadequacies in quality or manner of service delivery, supports this view[11]. The Supreme Court in *Indian Medical Association v. V.P. Shantha*[12] upheld that service under consumer law should be interpreted broadly to pursue additional remedial aims. In a broader sense, banks, fintech applications, and intermediaries have digital payment services, which fall under consumer jurisprudence. An ecosystem of payment that subjects users to avoidable cyber fraud or security breaches in the background can thus be considered a poor consumer service.

The ***Reserve Bank of India's Master Directions on Digital Payment Security Controls, 2021***[13]***,*** is a regulation that requires the entities to establish effective cybersecurity controls, fraud detection and prevention systems, along with secure authentication infrastructure.

Likewise, ***Section 8 of DPDP 2023***[14] has a mandatory provision that data fiduciaries have a duty to ensure reasonable security measures to avoid personal data breaches. These structures, when combined, suggest a regulatory change in the direction of the security of digital payments

[9] Organisation for Economic Co-operation and Development (OECD), *Consumer Policy and the Digital Transformation* (2018).
[10] National Payments Corporation of India (NPCI), *UPI Product Overview* (2024).
[11] Consumer Protection Act, 2019, No. 35 of 2019, §§ 2(11), 2(42), INDIA CODE.
[12] *Indian Medical Association v. V.P. Shantha (1995) 6 SCC 651 (India).*
[13] Reserve Bank of India, *Master Direction on Digital Payment Security Controls* (2021).
[14] Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 8, INDIA CODE.

being identified as part of consumer welfare.

2.2 Study of the Rise of UPI Fraud and Consumer Vulnerability

The increasing rate of UPI fraud is an example of why it is important to consider payment security as consumer safety. While digital payments remain highly secure on paper, fraudsters use newer and different methods to exploit people, especially elders and people with less digital knowledge, through psychological manipulation, leading to a "***5-fold jump***" in financial losses from 2022 to 2024, with a total reported loss exceeding ₹1000 crore[15][16]. These lead to structural vulnerabilities in authentication measures, fraud-detection systems, and the architecture of transaction monitoring of the existing security system.

For example, if a bank or a UPI app system allows an unauthorised transaction that fails to detect fraud will result in the consumer losing their hard-earned money. It's the responsibility of the bank or the UPI app company to provide compensation for a deficient consumer service because the payment service was delivered in an unsafe and inadequate manner.

2.3 Limitations of Traditional Consumer Redressal

Although digital payments are conceptually covered by the consumer protection law, conventional redressal mechanisms are structurally ill-equipped to handle payment fraud cases[17]. The **Consumer Protection Act** is mainly a law offering ex post remedial measures by complaints in **Section 35** and adjudication in **Section 38[18]**.

Indian consumer jurisprudence has traditionally placed a very strong emphasis on compensatory redress once the injury has taken place, as acknowledged in *Lucknow Development Authority v. M.K. Gupta[19]*.

But this type of post-hoc adjudication is not well adapted to the digital payment battle, where the damage is done immediately, and quick action is usually necessary to provide relief. Moreover, even though the consumers cannot access the backend technical data, fraud-

[15] Reserve Bank of India, *Annual Report 2023–24* (2024).
[16] Ministry of Finance, Govt. of India, *Cyber Fraud and Digital Payment Security Data* (2024).
[17] Reserve Bank of India, *Customer Protection—Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*, RBI/2017-18/15.
[18] Consumer Protection Act, 2019, No. 35 of 2019, §§ 35, 38, INDIA CODE.
[19] *Lucknow Development Authority v. M.K. Gupta (1994) 1 SCC 243 (India).*

detection logs, or authentication records, they have significant evidentiary burdens. The liability is also spread among the banks, gateways, aggregators, and processors, and each might refuse to have any responsibility[20]. As a result, theoretically, statutory remedies are available, but they turn out to be timely or technically ineffective.

These restrictions make it clear that digital payment fraud, in the theoretical sense of a consumer protection issue, cannot be sufficiently handled by ex post remedies of the public law alone, but rather requires the focus on the contractual arrangements that operationalise the concept of payment security privately.

CONTRACTUAL ARCHITECTURE OF THE FINTECH ECOSYSTEM

Online transactions of payments are no longer two-way payments between a bank and a consumer[21]. Contemporary payment apps are built on a multiple-tier fintech stack with banks, payment gateways, payment aggregators, cloud-service providers, fraud-detection and authentication intermediaries[22]. The consumer only interacts with the payment app or the bank, but the security of the transaction is reliant upon contractual relationships with these backend entities, all of whom have a critical operational or technological role to play[23].

The digital payments with respect to consumer safety is dependent on a network of inter-institutional contracts to which the consumer is not part of[24] ***Section 43A*** of the ***IT Act***[25], which provides some regulation of this architecture, and the ***RBI Cyber Security Framework***[26] under ***Payment and Settlement Systems Act, 2007***[27], which mandates regulated entities to have strong cybersecurity controls and oversight over vendors, partly govern this architecture. Nevertheless, these frameworks lack a thorough application of liability throughout the fintech chain, with the contractual arrangements defining the risk allocation and responsibility.

- Case Study of the Cosmos Bank Cyber Heist (2018)

The systemic nature of digital payment risk can be shown in this case, during which a set of

[20] Reserve Bank of India, *Framework for Strengthening the Resilience of Digital Payment Systems* (2021).
[21] National Payments Corporation of India (NPCI), *UPI Ecosystem Overview* (2024).
[22] NASSCOM, *Cybersecurity in Digital Payments Ecosystem* (2023).
[23] Organisation for Economic Co-operation and Development (OECD), *Digital Security Risk Management* (2019).
[24] NASSCOM, *Model Technology Contract Clauses* (2024).
[25] Information Technology Act, 2000, No. 21 of 2000, § 43A, INDIA CODE.
[26] Reserve Bank of India, *Cyber Security Framework for Banks* (2016).
[27] Payment and Settlement Systems Act, 2007, No. 51 of 2007, INDIA CODE.

malware targeted the ATM switch infrastructure of the bank, stealing around ₹94 crore[28]. The accident was due to institutional and technological failures in the back end[29]. However, the loss to consumers and disruption to the system cascaded out of system weaknesses in the payment chain, a demonstration of how the damage of digital payments is often more due to infrastructural failure than individual wrongdoing.

4. CONTRACTUALISATION OF PAYMENTS SECURITY.

4.1 From Public Regulation to Private Governance

In India, the security of digital payments has shifted to the mode of delegated governance of contracts rather than being a direct regulatory enforcement[30]. ***The Master Direction of the RBI on Cyber Resilience and Digital Payment Security Controls, 2024***[31], requires *Payment System Operators (PSO's)* to make sure that the unregulated partners comply by mutual agreement, which basically imposes regulatory duties upon them by private contract.

Under this new framework, contracts act as regulators' surrogates in enforcing compliance via audits, indemnity, and service-level agreements, all with a high level of penetration in the fintech stack[32]. However, this development alters the source of consumer protection, moving from statutory safeguards to contractual arrangements between institutions.

A feeble audit provision or an inadequately written indemnity will not be a secret failure; it will become a systemic weakness to the consumers, as their data and finances are endangered even with the presence of formal regulatory compliance.

4.2 Cascading Liability Chain and Privity Gap.

Digital payments architecture demonstrates a chain of liability: consumer-bank-aggregator-gateway-vendor[33]. This arrangement causes a privity gap, in which the consumer is at a loss and does not have a contractual relationship with the party at fault[34].

[28] Brian Krebs, *Indian Bank Hit in $13.5M Cyberheist*, Krebs on Security (Aug. 17, 2018)
[29] Indian Computer Emergency Response Team (CERT-In), *Cyber Security Incident Reports* (2018–19).
[30] OECD, *Digital Security Risk Management for Economic and Social Prosperity* (2019).
[31] Reserve Bank of India, *Master Direction on Cyber Resilience and Digital Payment Security Controls* (2024).
[32] *Supra,* Note 24.
[33] *Supra,* Note 22.
[34] *Id.*

The Supreme Court's decision in *M/s Citicorp Finance v. Snehasis Nanda*[35] (2025) underscores that the burden of proving a tripartite contractual relationship lies on the party asserting it. However, in online transactions, no such relationship tends to be established, which results in what can be called a *'contractual black hole',* where liability is diffused across multiple actors without clear accountability.

The ***RBI Authentication Mechanisms Directions, 2025***[36]***,*** which adds risk-based authentication, adds to this obscurity. In such cases, approval of the transaction relies on algorithmic evaluations by third-party vendors.

In case of failure of such systems, liability is not defined by statute but by inter-institutional contracts, which place consumers in a remedial uncertainty, even with the increased access to consumer forums, which are acknowledged by the Supreme Court (2026)[37].

4.3 Invisible Adhesion Contracts as a matter of Consumer Protection.

Consumer protection in digital payments operates through **"invisible" standard form contracts**, to which the consumer is not a party[38].

"The consumer's digital safety is a third-party beneficiary of a private bargain they never signed."- Lina Khan.[39]

These contracts represent a shadow regulatory regime, which apportions risk to the "least cost avoider" of risk via indemnity clauses and service-level agreements[40]. Nevertheless, there has been a rising trend in courts stepping in where such contractual agreements are infringing the rights of consumers.

It was restated in *Roopam Kumar v. SBI Cards* (2026)[41] that the liability is on the bank to establish customer negligence, and the liability cannot be contractually transferred. Similarly,

[35] *M/s Citicorp Fin. (India) Ltd. v. Snehasis Nanda*, (2025) 3 S.C.R. 866 (India).
[36] Reserve Bank of India, *Authentication Mechanisms Directions* (2025).
[37] *Supra*, Note 3.
[38] Santhosh S. & Dr. J.S. Senthil Kumar, *Unfair Terms in Standard Digital Contracts: A Hidden Threat to Human Rights and Consumer Justice*, International Journal of Research Publication and Reviews (IJRPR) (2026), https://www.researchgate.net/publication/399482062.
[39] Statement of Chair Lina M. Khan Regarding the Matter of Avast, Federal Trade Commission (Feb. 22, 2024)
[40] Friedrich Kessler, *Contracts of Adhesion—Some Thoughts About Freedom of Contract*, 43 Columbia Law Review 629 (1943).
[41] *Roopam Kumar v. SBI Cards & Payment Servs. Pvt. Ltd.*, Consumer Complaint No. DC/AB1/44/CC/255/2021 (Dist. Consumer Disputes Redressal Comm'n-II, Chandigarh, Feb. 6, 2026) (India).

in *Jaiprakash Kulkarni v. Bank of Baroda* (2024)[42], the Bombay High Court maintained that consumers are not liable to any third-party breach within the system.

The doctrine of unconscionability, established in *Central Inland Water Transport Case*[43], further limits the enforceability of one-sided fintech terms. This is reinforced by *M. Hemalatha Devi v. B. Udayasri* (2024)[44], where arbitration clauses in adhesion contracts were held insufficient to oust consumer jurisdiction.

Interestingly, although the ***DPDP Act, 2023***[45] protects personal information, the monetary liability is regulated through the contract law, which exposes a two-system regime, in which the law secures data, whereas money secures contracts.

5. REGULATORY COMPARISON

5.1 The "Reimbursement Revolution": India and the UK.

The regulation of digital payments in jurisdictions is an obvious transfer of the responsibility of the user to the institutional liability[46]. In India, the changing zero-liability system by the RBI lays the burden on banks whereby unauthorised transactions are reported in time, which is contrary to the traditional principle of caveat emptor[47].

In the United Kingdom, the more explicit model is available. *Payment Systems Regulator (PSR)* has required *Authorised Push Payment (APP)* fraud to be reimbursed since October 2024, usually apportioning liability between sending and receiving banks on a 50:50 ratio[48].

Although the primary bank is a central organiser of liability in India and institutions in the UK, both systems represent a common normative reorientation:

"Caveat Emptor to Caveat Vendor"[4950]***.***

[42] *Jaiprakash Kulkarni v. Banking Ombudsman*, 2024 SCC OnLine Bom 1666 (India).
[43] *Supra,* Note 8.
[44] *M. Hemalatha Devi v. B. Udayasri*, (2024) 4 S.C.C. 255 (India).
[45] *Supra,* Note 5.
[46] World Bank, *Payment Systems Worldwide: A Snapshot* (2022).
[47] *Supra,* Note 17.
[48] Payment Systems Regulator (U.K.), *APP Reimbursement Requirement* (2024).
[49] E.B. Weiss, *Consumerism and Marketing: Part II—From Caveat Emptor to Caveat Vendor*, Advertising Age, May 15, 1967, at 92.
[50] *M/S Indsil Hydro Power & Manganese Ltd. v. State of Kerala*, (2021) 10 SCC 165 (India).

5.2 Open Finance Security: India's AA vs EU's FiDA

The growing open finance presents new data sharing and payment authorisation risks[51]. The ***Account Aggregator (AA) structure*** in India exemplifies one of the best models of consent-by-design, which allows access to data in a granular, revocable and auditable manner[52].

The new ***FiDA Regulation (2025-2026)*** suggested by the European Union, and the reform of ***PSD3***, has a broader scope, but it is serious in its innovation: strict liability in cases of impersonation fraud[53]. In cases where users are misled by spoofing or a false representation, the institutions may be liable regardless of whether the user is authorized or not.

This is a major deviation. India places more emphasis on consent architecture as compared to the EU which places greater emphasis on institutional accountability in deception-based fraud. Since there is now the emergence of vishing, deepfakes and a so-called digital arrest scam, the addition of spoofing liability to Indian laws would reinforce consumer protection to its contractual framework[54].

5.3 Fraud Response in Real-time: UPI vs Pix.

Liability defines who pays, whereas response systems define how quick recovery is achieved. The UPI ecosystem in India is facilitated by ***CFCFRMS***, and ***1930 helpline***, but lacks automated coordination, resulting in critical delays[55].

The Pix system used in Brazil, on the other hand, has a *Special Return Mechanism (MED)* that allows almost instant blocking of accounts and recovery of funds through automated inter-bank protocols[56]. It is evident that there is an area of concern here, as India has advanced infrastructure, while Brazil exhibits more contract integration for real-time compliance.

6. CRITICAL ANALYSIS: CONSTRAINTS OF CONTRACTUAL PROTECTION.

6.1 The Unconscionability Paradox

[51] Financial Stability Board, *Open Finance: Policy Considerations* (2022).
[52] Reserve Bank of India, *Account Aggregator Framework* (2021).
[53] European Commission, *Financial Data Access (FiDA) Proposal* (2023).
[54] European Central Bank, *Payment Services Directive 3 (PSD3) Proposal* (2023).
[55] National Payments Corporation of India (NPCI), *UPI Fraud Monitoring Framework* (2023).
[56] Central Bank of Brazil, *Pix Special Return Mechanism (MED)* (2022).

The unconscionability doctrine, as established in C*entral Inland Water Transport Corporation v. Brojo Nath*[57], is pertinent when evaluating fintech contracts based on unequal bargaining positions. The modern application of this doctrine can be seen in click-wrap contracts, which are standardized and non-negotiable terms that grant access to vital payment systems[58].

This leads to a structural contradiction. On the one hand, the ***Digital Personal Data Protection Act, 2023***[59] mandates that consent must be both informed and meaningful in any data processing exercise.

On the other hand, the contractual agreement exonerates the party from liability for failure to fulfil its obligations due to a problem with the technology used or a breach by a third party. Consent is regulated, whereas contract law is not.

6.2 The Black Box Problem: Algorithmic Unconscionability.

Systems utilising *Risk-Based Authentication (RBA)* rely on the automation of decisions, regarding whether the transaction should be approved or disapproved, using proprietary algorithms that use behavioural and Device-based data to reach such conclusions[60].

The consequence of this system is an inherent lack of due process for consumers. When fraud is committed because of errors within the algorithm used for authentication or assessment of the risk involved, consumers have no chance to investigate such a decision, since algorithms are protected from disclosure by trade secrets law[61].

6.3 The Enforcement Gap: Sandboxes and Real- World Harm.

Regulatory sandboxes, like the ***2026 IFSCA framework***[62], allow people test new financial products in a reliable manner, which encourages innovation. Nevertheless, they produce a vacuum of liability as well. This is because the users involved in testing a live setting might not have the same contractual protection as the ordinary consumer, although they are exposed

[57] *Supra,* Note 8.
[58] *Supra,* Note 40.
[59] *Supra*, Note 5.
[60] OECD, *Artificial Intelligence in Finance* (2021).
[61] Arnis Prazulis, *Legal Implications of Automated Suspicious Transaction Monitoring*, J. Banking & Fin. Tech. (2024).
[62] International Financial Services Centres Authority (IFSCA), *Regulatory Sandbox Framework* (2026).

to actual financial risks.

This is an underlying conflict: even though sandboxes can speed up technology creation, they are also likely to create second-class consumers, since they will be disproportionately risky in the name of innovation.

6.4 Insolvency Risk in the payment chain.

Consumers are also subjected to some intermediary insolvency risk due to the contractual nature of digital payments[63]. When a Payment Aggregator or Gateway malfunctions, consumer funds are at risk according to contractual requirements on fund segregation.

Consumer law frameworks are silent when it comes to such cases even though emerging regulatory attention has been raised. As a result, contractual opacity transfers financial risk to the consumers, when they are not in control of the solvency of intermediaries.

-The New Social Contract.

"*The safety of digital payments is no longer a two-way agreement between a bank and its customer: it is a* **risk-sharing ecosystem"- *T.Rabi Sankar***[64].

"Consumer protection" itself cannot be the future of consumer protection, but making sure that the risks of contractual governance are fairly spread throughout the ecosystem, and not imposed on the most uninformed member without a murmur.

7. REFORM PROPOSALS

The digital payments framework in India needs to actively regulate the private infrastructure that now delivers consumer protection rather than passively acknowledging contractual governance[65].

Firstly, the Reserve Bank of India should impose minimum cybersecurity and liability-allocation clauses in all fintech and payment-intermediary contracts, ensuring a common

[63] Reserve Bank of India, *Guidelines on Payment Aggregators and Payment Gateways* (2020).
[64] T. Rabi Sankar, Deputy Governor, Reserve Bank of India, Keynote Address at the Global Fintech Fest, Mumbai: *Fintech Innovation and Approach to Regulation* (Sept. 5, 2023).
[65] Reserve Bank of India, *Payment and Settlement Systems in India: Vision 2025* (2022).

baseline that applies across the ecosystem.

Secondly, there should be a ***statutory spoofing and impersonation fraud liability regime*** under Indian law on the lines of emerging European frameworks[6667]. So consumers are misled by novate setup fraud through technological sophistication, requiring presumptive institutional liability.

Thirdly, algorithmic fraud-detection systems and risk-based authentication systems should be subject to ***auditability and explainability requirements***, to prevent "black-box" decision-making that may undermine accountability.

Ultimately**,** ***stronger fund-segregation and insolvency-protection norms*** must be imposed on payment intermediaries and aggregators to safeguard consumers from backend institutional collapse.

8. CONCLUSION

In conclusion, digital payment safety can neither be understood as a bilateral bank-customer issue. Rather, it is the result of a multilayered ecosystem of contracts that allocate the risk privately across the fintech chain[68]. Due to the complicated nature of digital payments, contractualization cannot afford to become unnoticeable but should be regulated. Although supplementing public law, private contracts must not obscure liability or allow the externalisation of systemic risk on consumers. According to the authors, consumer protection in digital finance will not come from replacing regulations with contracts, but rather ensuring that the governance of contracts is publicly monitored, visible, and organised around the proposition that the party best placed to prevent digital harm bears its costs. Only then can India truly achieve the vision of ***safe products and confident consumers***.

[66] Commission Proposal for a Regulation of the European Parliament and of the Council on a Framework for Financial Data Access, COM (2023) 360 final (June 28, 2023).
[67] Commission Proposal for a Directive of the European Parliament and of the Council on Payment Services and Electronic Money Services in the Internal Market, COM (2023) 366 final (June 28, 2023).
[68] Bank for International Settlements, *Sound Practices: Implications of Fintech Developments for Banks* (2018).