The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

ARTICLE: DIGITAL PAYMENTS SECURITY LAWS

~ RANVEER SINGH TANWAR

INTRODUCTION: WHEN THE MACHINE SAYS YES BUT THE CONSUMER SAYS NO

Someone calls claiming to be from a bank. The voice is convincing, the caller knows the last 4 digits of the account and there is enough urgency in the conversation, that the threat appears to be real: verify immediately, or the account will be blocked. A few minutes later, the money is gone. But the transaction record has a much different story. The correct credentials were used. The OTP was entered. The payment was successfully verified.

For the bank's system, there may be nothing unusual about this transaction. If the individual has lost the funds, it is obvious that it is a scam. The law is somewhere in between these two renditions of the same event.

The question is one that is very hard to answer in the world of digital payment security today. India's payment system has turned into a remarkable machine at determining if the right PIN, password or OTP was provided. It is much less clear if the question is whether the person entering it really intended the transaction that ensued. This distinction matters because fraud itself has evolved. Being a criminal doesn't require necessarily hacking into a bank's servers or a password. In some cases, it is sufficient to make the victim feel the need to trust them, to make them feel like there's been a serious emergency, or to successfully mimic a familiar voice so that the victim will go through with the transaction on their own.

Indian law doesn't attempt to solve this issue in a single act. The Payment and Settlement Systems Act 2007 has put payment systems under the regulatory control of the Reserve Bank

of India[1]. The Information Technology Act, 2000 provides for dealing with the problem of identity theft, cheating through personation and some failures in the context of electronic data. In addition to the remedies provided by consumer protection law, India's data protection law also imposes obligations on banks with regard to the security of personal data. In addition to these laws, there is a huge regulatory infrastructure set up by the RBI[2].

So, the challenge isn't that India doesn't have a law pertaining to digital payments. It has several. The more serious issue is whether the various legal principles yield a definite result at the crucial time: when the fraudulent payment has been actually made, who is to suffer the loss?

This article contends that India's digital payment framework needs to move beyond an almost binary understanding of bank fault and customer negligence. However, authentication is not always a secure basis for meaningful authorisation, especially when fraud has evolved into a tactic of exploiting consent, not bypassing or defeating technology. Existing law doesn't resolve another question that needs to be addressed in the next generation of payment regulation: who to believe if payments are recorded on the machine and the person says they were misled - the machine or the human being?

INDIA'S DIGITAL PAYMENT LAW: A FRAMEWORK BUILT IN FRAGMENTS

The legal journey of a digital payment does not start and end with one statute. The same transaction could concurrently be subject to banking regulation concerns, cybercrime concerns, consumer protection concerns, data security and electronic evidence concerns. This multi-layered approach has enabled the Indian regulators to keep up with the advances in technology without having to wait for a new law for each payment method. It has also given rise to an interesting situation, however: a fraudulent transaction could fall under a number of laws, none of which would give a complete answer as to who has to bear the loss[3].

The Payment and Settlement Systems Act, 2007 is the key in the regulatory framework. Section 4 bars operation of any payment system without RBI's authorization, and sections 10 and 18 provide enough power to the central bank to set standards and make directions about the

[1] Payment and Settlement Systems Act, No. 51 of 2007, §§ 3–4, India Code (2007)
[2] Reserve Bank of India, *Customer Protection—Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*, RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017)
[3] Shehnaz Ahmed & Aryan Babele, *Modernising the Law for Payment Services in India: Preparing for the Future of Retail Payments* 8–15 (Vidhi Ctr. for Legal Pol'y 2021)

payment systems[4]. The Act is however more in nature of regulation. It sets out who would be allowed to run a payment system and how payment systems can be supervised, but provides no comprehensive statutory regime for distributing losses between banks and consumers across different forms of digital fraud.

That has therefore been passed on to the RBI. It was in 2017 when it launched the circular on protection of customers in unauthorised electronic banking transactions, which implemented the concept of a 'graded liability'. If the fault is with the bank, a customer could be held responsible for nothing regardless of when he/she reports the fraud. In some third-party cases, if the customer notifies the bank within 3 working days of any communication regarding an unauthorised transaction, then there is a possibility of zero liability. If the loss is caused by the customer's own negligence, however, the customer will have to cover the loss until a report is made on the unauthorised transaction[5].

It is here that the problem of fraud becomes "uncomfortable" under the law. What exactly should be considered customer negligence? The easy case would be where a person knowingly shares an OTP despite repeated warnings. However, the answer is less clear when the deception is through a spoofed call or person with a fake voice, when the person's personal information has been deceptively acquired or when the impersonator has some personal information that should only have been available in a trusted institution. If all disclosures of credentials are considered the same, the law may not differentiate between careless and more deceptive disclosures.

The Information Technology Act, 2000 takes a different approach to the transaction however. Sections 66C and 66D criminalise identity theft and cheating by personation through computer resources[6]. But it does not necessarily solve the victim's short-term civil dilemma of recovery of the stolen money (if one can even be identified). There is a relationship between criminal liability and loss allocation but it is not an equivalence.

Partly this is occupied by consumer law. If a bank or payment service provider does not implement reasonably adequate protections, does not respond promptly to an individual's complaint of fraud, or does not follow payment service provider-specific binding regulations

[4] Payment and Settlement Systems Act, No. 51 of 2007, §§ 4, 10, 18, India Code (2007)
[5] Reserve Bank of India, supra note 2, ¶ 6
[6] Information Technology Act, No. 21 of 2000, §§ 66C–66D, India Code (2000)

issued by the Department, it may be a deficiency in service under the Consumer Protection Act, 2019[7]. There's one more layer of data protection. If the information stolen from a person allows for effective impersonation or compromising of the account, then not only does the question of how the crime was committed arise, but whether some entity in the data chain did not implement the required level of security as required by law.

India, thus, cannot be accused of having no legal rules governing digital payments. The real difficulty is that responsibility is spread across them. There is one law that is about the payment system, a second law that is about the deception and a third that is about the consumer, and regulations provide directions as to liability in certain circumstances. The fraud, on the other hand, occurs just once. For the victim, however, the question remains painfully simple: who gives the money back?

AUTHENTICATION IS NOT ALWAYS AUTHORISATION: THE CENTRAL LEGAL PROBLEM

Conventionally, payment security depended on a fairly straightforward premise: If the correct password, PIN or OTP was entered, there was good reason to believe that the account holder had authorised the transaction. That assumption made sense when fraud largely meant stolen cards, hacked accounts or compromised credentials. It is even more difficult to defend if the fraudster does not attempt to break into the security system, but instead gets the victim to open the door.

Imagine a person enters a UPI PIN when he is told to do so in order to get a refund. Or a person who seems to be a member of your family, but is actually a clone from the AI. In both cases, the payment may be technically genuine in the narrowest sense, that is, the actual account holder used the right device and credentials. However, the intent behind the act was created with deception. The system is used to verify the identity of the individual, not necessarily the reality from which the individual made his decision.

While Indian banking regulation does not completely overlook consumer deception, the liability provisions are still largely predicated on the differences between institutional fault, third-party breach, and customer negligence. As per the RBI's 2017 circular, if the loss is a

[7] Consumer Protection Act, No. 35 of 2019, §§ 2(11), 2(42), India Code (2019)

result of neglectful sharing of payment information by the customer, the customer would be responsible for the loss till the unauthorised transaction is reported[8].

However, the circular leaves a more difficult question unanswered as to whether, if sophisticated deception is used, placing the required credential by the customer in the hands of the bank constitutes an "unauthorised electronic banking transaction" under the liability provisions? The logic in this is not that the Indian banking law already deems all payments made as a result of fraud to be unauthorised. It is that the existing categories become less certain where technical authentication and genuine transactional intent begin to diverge.

This is where the distinction between authentication and authorisation should be looked at. Authentication resolves the question of whether the credential prescribed was used. Authorisation is a harder question: Was there any actual authorisation of the transaction? These two things often overlap, but modern social-engineering fraud proves they can be different.

This principle of consent, although not directly applicable, provides a helpful analogy[9]. Under section 17 of the Indian Contract Act, 1872, fraud includes certain acts of deception intended to induce another person to enter into a contract. Section 19 acknowledges that an agreement may be voidable if there has been a fraud or misrepresentation that has caused the consent. These provisions do not necessarily apply in a contractual relationship between the victim and fraudster in the traditional sense, and cannot be readily transferred into banking regulation. The principle of the law, however, is hard to miss: Law has long accepted that an outwardly voluntary act may not be a true act of consent when it has been the result of deception.

The problem is complicated by the fact that today's fraud-risk algorithms can, under certain conditions and depending on how they are designed, detect cues like unusual devices, abnormal amounts of transactions or major deviations from transactional patterns. So, this is another legal question. Should a correct OTP or PIN automatically end the inquiry if an institution possesses the technological capacity to detect a seriously anomalous transaction but fails to act on obvious warning signs?

The solution does not lie in allowing a reimbursement without any consideration of conduct to all consumers who have been deceived. This kind of rule might lead to the development of

[8] Reserve Bank of India, supra note 2, ¶ 6(iii)
[9] Indian Contract Act, No. 9 of 1872, §§ 13–14, 17, 19, India Code (1872)

carelessness and real evidence problems. The other end of the spectrum is equally bad though. The law has the potential to put the whole responsibility for ever-fancier frauds into the hands of the party who is least able to determine how the fraud was constructed.

What is needed, therefore, is not the disappearance of customer responsibility, but a more nuanced legal test. The sophistication of the deception, precautions taken by the consumer, security architecture of the institution, availability of warning signs and speed of reporting should all be taken into consideration. Today, when nothing can be trusted, and when it's possible to impersonate a business and its interactions via deepfakes, the question should no longer be if the customer hit the button. It also should be determined if the law has a sound basis to regard that action as a bona fide taking of financial risk.

FROM FRAGMENTED REMEDIES TO A FAIRER LIABILITY STANDARD

When it comes to digital payment fraud, it's most apparent once the payment has been made. The victim can go to the bank, file a complaint with the cybercrime mechanism, file a complaint with the bank's regulatory grievance committee and/or seek relief, as applicable, in consumer law. Yet the existence of several remedies does not necessarily produce a clear principle for deciding who should ultimately bear the loss.

The RBI has now come up with its 2017 circular in an effort to provide some clarity on the issue[10]. It means that if the unauthorised transaction is due to fraud, negligence or deficiency by the bank, then there is no liability of the customer. If the failure is not of the bank or the customer, but somewhere else in the system (third party), then there may also be no liability, if the customer reports the transaction within three working days since he received the notification thereof. Importantly, the burden of proving customer liability rests upon the bank[11].

The case of State Bank of India v Pallabh Bhowmick is a good example of the significance of the framework. The fraudsters had convinced the customer to download an app on his mobile phone and then ₹94,204.80 was deducted from his account. The Gauhati High Court had concluded that the transactions were unauthorised and fraudulent, the customer had timely informed the bank about such transactions and the bank had failed to prove negligence on the

[10] Reserve Bank of India, supra note 2, ¶¶ 6–12
[11] *Id.* ¶ 12

customer's part. Ultimately, SBI's challenge went to the Supreme Court, which on 3 January 2025 refused to intervene in the High Court's order[12].

The case study is important but its scope is equally important. It doesn't mean that all customers fooled into making a fraudulent transaction are guaranteed a reimbursement. Nor does it resolve the more difficult question that lies at the heart of today's social engineering fraud: what if the customer has entered the required PIN/OTP or other credential himself, but the decision that was made was deceptive?

Here, the present liability structure must be made more complex. The discussion simply reduces to two opposing claims: The bank claims, "Valid credentials were used" and the customer claims, "It was fraudulent". Both facts should not automatically be final answers to the question. A reasonable contextual fraud definition should look at the sophistication of the fraud, the actions of the consumer, whether the institution was doing everything it should to prevent and/or contain the loss, whether the transaction was anomalous, whether the institution was quick to report it, etc. and whether either party could reasonably have averted or contained the loss.

If this were the standard, then there would be no guarantee of reimbursement if there were any allegations of deception. Nor should it[13]. But it should not be a burden upon the legal investigation to be over once the correct PIN/OTP has been entered. The behaviour and security measures of the payment provider need to be included in the assessment of the liability in the case where warning signs can be identified.

There's also a greater issue of velocity. Money can move through several accounts within minutes, while determining liability and obtaining reimbursement may take months or even years. There is, therefore, a need for clarity on responsibilities to fast-track trace and freeze suspected proceeds of crime, keeping of proper transaction records and timely exchange of information between banks, payment intermediaries and investigative agencies[14].

Finally, digital payment law must move beyond asking only who entered the credential. It ought also to question who was in the best position to prevent the loss, to detect what the

[12] *State Bank of India v. Pallabh Bhowmick*, W.A. No. 364/2022 (Gauhati H.C. Sept. 13, 2024); *State Bank of India v. Pallabh Bhowmick*, S.L.P. (C) No. 30677/2024 (India Jan. 3, 2025) (order)
[13] *See* Reserve Bank of India, supra note 2, ¶¶ 6–9
[14] *See generally* Shehnaz Ahmed & Aryan Babele, supra note 3

anomaly was and to make sure that the money didn't go any further. That's a more challenging inquiry than to automatically assume it's either the bank or the consumer. It's also much more similar to the way real-life fraud works.

CONCLUSION: A PAYMENT SYSTEM IS ONLY AS SECURE AS ITS REMEDY

The digital payment narrative of India can be told in terms of numbers - billions of transactions, growing UPI usage and money being moved within seconds. But, the real determining factor of a payment system is when something goes wrong.

With the advent of modern fraud, it's not so much about defeating the authentication; it's about manipulating the individual being authenticated. That shift has revealed a gap in the law which continues to apply a broad definition of institutional fault and customer negligence to determine responsibility. Digital payment law should take into account that a transaction may be technically valid but be the result of a clever deception.

This does not mean banks need to be insurers of all fraudulent losses or to shift the burden of reasonable caution to consumers. What's needed is a more balanced approach - a liability model that can consider the manner in which the fraud took place, what each party could reasonably have done to stop it, whether warning signs were missed and how fast institutions responded when they were alerted to the fraud.

India has created a payment system, where funds can flow across the country almost instantaneously. Its next legal challenge is to ensure that if fraud can travel at such speed, responsibility does not take years to catch up.