

**BEFORE THE ADJUDICATING OFFICER**

SECRETARY,
ELECTRONICS, INFORMATION TECHNOLOGY & ARTIFICIAL INTELLIGENCE DEPARTMENT,
MANTRALAYA, MUMBAI, MAHARASHTRA.

UNDER THE INFORMATION TECHNOLOGY ACT, 2000

IN

COMPLAINT CASE NUMBER 01 OF 2019

क्र.मातंसं-7519/प्र.क्र.3/(1/2018)से-2/39

Reserved on: 30.07.2026

Pronounced on: (Date of Digital Signature)

IN THE MATTER OF,

Bharat Jyoti Impex

) ... Complainant

VERSUS

IDFC Bank

) ... Respondent

Appearances:

Adv. G. Krishna Mohan Nair, o/b/o. Complainant;

Adv. Parikshit Desai, i/b. SNG & Partners, o/b/o. Respondents.

[This document presents the proceedings of a complaint filed by the Complainant for adjudication under Section 46 of The Information Technology Act, 2000 (as amended in 2008) (referred to as the "Act"). The hearings were conducted in accordance with the principles of natural justice and reasonable opportunity, ensuring that both parties, namely the Complainant and the Respondents, were given equal and sufficient opportunities to present and defend their respective cases. After the conclusion of the hearings and the receipt of responses from all involved parties, a decision has been reached, and this judgment is now being delivered.]

I. THE BRIEF FACTS OF THE CASE, AS STATED BY THE COMPLAINANT, ARE AS FOLLOWS:

1. The present Complaint has been instituted by **M/s. Bharat Jyoti Impex**, a proprietary concern carrying on business in import, export and trading activities from its office situated at Jasu Building, 30, Dadabhai Road, Vile Parle (West), Mumbai. The Complainant maintains a **Current Account bearing No. 10011804744** with the Respondent Bank, namely **IDFC Bank Ltd., Naman Branch, Bandra Kurla**

Complex, Mumbai, through which it regularly conducted its banking operations, including high-value electronic fund transfers. The Complainant has approached this Authority under Section 46 of the Information Technology Act, 2000 alleging negligence and failure on the part of the Respondent Bank in processing unauthorized electronic banking transactions.

2. Learned Counsel appearing on behalf of the Complainant Mr. G. Krishna Mohan Nair submitted that the office of the Complainant remained closed on account of the Diwali holidays from **06.11.2018 to 11.11.2018**. Upon resumption of business on **12.11.2018**, the Complainant discovered that a series of unauthorized **Real Time Gross Settlement (RTGS)** transactions had been executed from its Current Account during the aforesaid period, without the knowledge, authorization or consent of the Complainant.
3. It is the specific case of the Complainant that during the period between **06.11.2018 and 12.11.2018**, a total amount of **Rs.1,26,00,000/- (Rupees One Crore Twenty-Six Lakhs Only)** was fraudulently transferred from its account through **twelve (12) RTGS transactions** in favour of various third-party beneficiary accounts. According to the Complainant, these transactions were never initiated, authorized or approved by any of its partners or authorized signatories.
4. Learned Counsel for the Complainant further submitted that immediately upon discovering the unauthorized debit transactions on **12.11.2018**, the Complainant promptly informed the Respondent Bank through electronic mail requesting immediate stoppage, recall and reversal of the impugned RTGS transactions. The Complainant simultaneously addressed written communications to the Respondent Bank protesting the unauthorized transfers and categorically denying issuance of any instructions authorizing such transactions. Copies of the relevant communications have been placed on record.
5. It is further submitted that the Complainant lodged a written complaint before **Juhu Police Station, Mumbai**, and reporting commission of cyber fraud and requesting initiation of criminal proceedings against the unknown perpetrators responsible for siphoning funds from its bank account. Subsequently, an FIR bearing No. (556/2018) came to be registered and investigation was undertaken by the concerned police authorities. The Complainant contends that the prompt lodging of the complaint clearly demonstrates that it had neither participated in nor authorized the impugned electronic transactions.

6. Learned Counsel submitted that despite receiving immediate intimation regarding the fraudulent transactions, the Respondent Bank failed to exercise due diligence expected of a scheduled commercial bank handling high-value electronic fund transfers. It is alleged that the Bank neither recalled all the fraudulent transactions in time nor implemented adequate safeguards to prevent further transfers, thereby permitting the unauthorized debits to continue despite several warning indicators.
7. The Complainant further contends that the Respondent Bank processed the disputed RTGS transactions solely on the basis of email communications allegedly received from the registered email address of the Complainant. According to the Complainant, no authorized representative of the firm had issued such emails, nor had the Complainant executed or submitted the RTGS request forms relied upon by the Respondent Bank. It is submitted that the alleged emails were forged, fabricated and fraudulently generated by unknown persons, and therefore could not have constituted valid banking instructions.
8. Learned Counsel for the Complainant argued that before processing any high-value RTGS transaction in favour of newly added beneficiaries, the Respondent Bank was under an obligation to verify the authenticity of the transaction requests by adopting appropriate security measures, including customer verification, confirmation of beneficiary addition, verification of email authenticity and compliance with applicable RBI guidelines governing electronic banking transactions. It is submitted that no such verification was undertaken in the present case
9. It is further submitted that despite repeated opportunities granted during the course of the proceedings, the Respondent Bank failed to produce several material records before this Authority, including the original RTGS request forms allegedly received from the Complainant, the original emails forming the basis of the disputed transactions, complete email headers, server logs, authentication records, internal approval trail, cyber security verification records and other contemporaneous electronic evidence necessary to establish the genuineness of the disputed transactions. According to the Complainant, the withholding of these documents raises a serious doubt regarding the legitimacy of the transactions and the manner in which they were processed.
10. Learned Counsel further submitted that although the Respondent Bank subsequently succeeded in recovering and crediting an amount of **Rs.68,94,000/-** to the account of the Complainant after intervention with the beneficiary banks, a sum of

Rs.57,06,000/- still remained unrecovered. The Complainant contends that the subsequent recovery of a part of the amount itself establishes that the disputed transactions were fraudulent and unauthorized in nature.

11. It is the specific contention of the Complainant that the Respondent Bank failed to maintain reasonable security practices and procedures while processing the impugned electronic fund transfers and acted negligently in executing high-value RTGS transactions on the basis of unauthenticated electronic communications without adequate verification. According to the Complainant, such acts and omissions constitute failure to exercise the standard of care expected of a banking institution entrusted with safeguarding customers' electronic banking transactions and thereby attract liability under the provisions of the Information Technology Act, 2000.
12. Learned Counsel concluded by submitting that the unauthorized electronic transfers resulted in substantial financial loss, disruption of the Complainant's business operations and deprivation of its legitimate funds. It is therefore prayed that this Authority hold the Respondent Bank liable for failure to maintain reasonable security practices and direct payment of appropriate compensation for the unrecovered amount together with such further reliefs as may be deemed fit and proper in the facts and circumstances of the present case.

II. SUBMISSIONS AND DEFENSES ADVANCED BY THE RESPONDENT

1. Learned Counsel appearing on behalf of the Respondent Bank strongly opposed the Complaint and submitted that the allegations levelled against the Bank are wholly misconceived, devoid of merit and liable to be dismissed. It is contended that the Respondent Bank had acted strictly in accordance with the banking mandate and the operational instructions furnished by the Complainant and that no negligence, deficiency in service or failure of security practices can be attributed to the Bank.
2. It is submitted that the disputed RTGS transactions were processed only after receipt of transaction requests through the registered email address of the Complainant. According to the Respondent, the transaction requests contained the requisite particulars and signatures corresponding with the records available with the Bank. The Bank, therefore, bona fide treated the said communications as valid customer

instructions and processed the RTGS transactions in the ordinary course of banking business.

3. Learned Counsel further submitted that the Complainant had voluntarily executed an Email Indemnity in favour of the Respondent Bank, thereby authorizing the Bank to process RTGS transactions received through the registered email address of the Complainant. It is contended that the Bank acted strictly in accordance with the terms of the said indemnity and the contractual arrangement existing between the parties.
4. It is the contention of the Respondent that the Bank had no reason to suspect that the email instructions received from the registered email account of the Complainant were unauthorized or fraudulent. According to the Respondent, the Bank cannot reasonably be expected to independently investigate the authenticity of every electronic communication where such communication originates from the customer's registered email address and bears the signatures available in the Bank's records.
5. Learned Counsel submitted that immediately upon receiving information regarding the disputed transactions, the Respondent Bank took prompt and appropriate steps by communicating with the beneficiary banks, initiating recall requests and freezing the beneficiary accounts wherever possible. As a consequence of these efforts, an amount of Rs.68,94,000/- was successfully recovered and credited back to the account of the Complainant. It is, therefore, submitted that the Bank acted diligently and in good faith immediately upon being notified of the alleged fraud.
6. The Respondent further contended that the primary cause of the loss suffered by the Complainant was its own failure to secure its registered email account and internal communication systems. It is submitted that if unauthorized persons gained access to the registered email address of the Complainant and transmitted fraudulent RTGS instructions, such compromise occurred entirely within the Complainant's electronic environment and was beyond the control of the Respondent Bank.
7. Learned Counsel further submitted that the Complainant admittedly received transaction alerts through SMS and email during the period in question but failed to take immediate corrective action. According to the Respondent, had the Complainant promptly informed the Bank immediately after receipt of the first transaction alert, several of the subsequent transactions could have been prevented. It is, therefore, contended that the Complainant substantially contributed to the loss by failing to exercise reasonable care and vigilance over its banking operations.

8. It is further submitted that despite alleging hacking and cyber fraud, the Complainant has not produced any forensic investigation report, cyber audit report or expert evidence establishing that its registered email account, computer system or electronic infrastructure had actually been compromised. In the absence of such evidence, the allegation that the disputed transactions resulted from hacking or cyber intrusion remains unsupported.
9. Learned Counsel also submitted that there has been no breach, compromise or unauthorized access to the Respondent Bank's Core Banking System, banking servers or electronic infrastructure. According to the Respondent, the entire banking platform remained secure throughout the relevant period and the impugned transactions were executed through the normal banking process after receipt of transaction instructions through the registered communication channel of the Complainant.
10. It is further contended that the provisions of Section 43A of the Information Technology Act, 2000 are not attracted to the facts of the present case since there has been no failure or breach of the Respondent Bank's computer system or electronic infrastructure. The Respondent submits that the alleged compromise pertains solely to the Complainant's registered email account and not to any deficiency in the Bank's information technology systems.
11. Learned Counsel finally submitted that the Respondent Bank has acted throughout in a bona fide manner, strictly in accordance with the contractual arrangements between the parties, established banking procedures and applicable regulatory framework. It is therefore prayed that the Complaint be dismissed with costs, as no negligence, failure of reasonable security practices or statutory liability can be attributed to the Respondent Bank on the basis of the material placed on record.

III. ISSUES & FINDINGS OF THE AUTHORITY

1. Reasonable and adequate opportunities were afforded to both the parties to present their respective cases. The matter was heard extensively over multiple hearings. This Authority has carefully considered the pleadings, documentary evidence placed on record, written submissions, rejoinders, oral arguments advanced by the learned Counsel appearing for the respective parties, and the material available on record before arriving at the present findings.

2. At the outset, it is observed that the Complainant has categorically stated that no parallel proceedings involving the subject matter of the present complaint are pending before any Court or competent adjudicatory forum so as to bar the jurisdiction of this Authority. The present complaint has been instituted under Section 46 of the Information Technology Act, 2000 seeking adjudication of compensation arising out of alleged unauthorized electronic banking transactions, and this Authority is therefore competent to adjudicate the present dispute.
3. From the pleadings of both parties, certain foundational facts remain undisputed. It is not disputed that the Complainant maintained **Current Account No. 10011804744** with the Respondent Bank. It is equally undisputed that between **06.11.2018 and 12.11.2018**, a series of RTGS transactions aggregating **Rs.1,26,00,000/-** were processed from the said account. It is further undisputed that, subsequent to the reporting of the incident, the Respondent Bank succeeded in recovering and crediting an amount of **Rs.68,94,000/-**, leaving a balance amount of **Rs.57,06,000/-** unrecovered. The principal controversy, therefore, is confined to the legality of the processing of the disputed RTGS transactions and the liability arising therefrom.
4. The principal defence raised by the Respondent Bank is that the disputed RTGS transactions were processed on the basis of electronic mail instructions allegedly received from the registered email address of the Complainant and in accordance with the Email Indemnity executed by the Complainant. However, during the course of the proceedings, this Authority specifically directed the Respondent Bank to produce the original RTGS request forms, the original electronic mail communications forming the basis of the disputed transactions, together with the supporting electronic records relied upon while processing the transactions. Despite such opportunity, the Respondent failed to place complete and satisfactory records before this Authority.
5. Significantly, the Respondent failed to produce complete electronic records including the original email headers, authentication logs, server logs, internal approval trail, system-generated audit records, maker-checker verification records and other contemporaneous electronic evidence capable of establishing that the impugned RTGS instructions were duly authenticated in accordance with the Respondent's internal security framework. In an electronic banking dispute where the authenticity of electronic instructions constitutes the very foundation of the defence, production of such primary electronic evidence assumes considerable importance.

6. The Respondent has relied substantially upon the Email Indemnity executed by the Complainant. However, the existence of such an indemnity, by itself, cannot absolve a banking institution of its independent statutory and regulatory obligation to maintain reasonable security practices while processing high-value electronic fund transfers. A contractual arrangement between the parties cannot dilute the standard of care expected from a scheduled commercial bank while dealing with electronic banking transactions involving substantial public funds.
7. The material placed on record further indicates that the disputed transactions involved transfer of an exceptionally large amount through multiple RTGS transactions to third-party beneficiary accounts within a short span of time. The Respondent has not produced any contemporaneous material demonstrating that additional verification procedures, enhanced authentication measures or internal risk assessment mechanisms were undertaken before processing such high-value transactions. In the absence of such material, the Respondent has failed to satisfactorily establish that adequate security measures were adopted while acting upon the disputed electronic instructions.
8. The Respondent has further contended that the compromise, if any, occurred in the registered email account of the Complainant and not within the banking infrastructure of the Respondent. However, irrespective of the origin of the fraudulent communication, the responsibility of independently verifying unusual, high-value electronic fund transfer instructions before permitting irreversible movement of customer funds cannot be completely shifted upon the customer. The duty to exercise reasonable care while processing electronic payment instructions continues to rest upon the banking institution entrusted with safeguarding customer accounts.
9. Nevertheless, the contributory conduct attributed to the Complainant does not exonerate the Respondent Bank from demonstrating that it had exercised the standard of care expected of a scheduled commercial bank while processing unusually large electronic transactions. The burden to establish compliance with reasonable security procedures rested upon the Respondent, particularly when the authenticity of the underlying electronic instructions was itself under challenge.
10. It is a settled principle that where a party having custody and control of the best available documentary and electronic evidence fails to produce the same despite specific directions of the adjudicating authority, an adverse inference may legitimately be drawn against such party. In the present proceedings, the Respondent

Bank failed to satisfactorily produce the foundational electronic records upon which its defence is founded which has been taken on record. Consequently, the Respondent has failed to discharge the burden of establishing that the impugned RTGS transactions were processed after due compliance with the applicable verification procedures.

11. Upon an overall appreciation of the pleadings, documentary evidence and submissions advanced by both sides, this Authority is satisfied that the Respondent Bank has failed to establish that reasonable security practices and due verification procedures were followed while processing the disputed RTGS transactions. The Respondent has also failed to satisfactorily explain the absence of the primary electronic records which alone could have conclusively established the authenticity of the disputed transaction instructions.

In light of the aforementioned findings, in my considered view, the Respondent Bank failed to demonstrate that the impugned electronic fund transfers were processed after adopting adequate verification mechanisms and reasonable security practices expected of a banking institution handling high-value electronic transactions. The failure to produce the foundational electronic records, coupled with the absence of satisfactory evidence demonstrating compliance with appropriate verification procedures, materially weakens the defence raised by the Respondent. Although the conduct of the Complainant in not acting immediately upon receipt of transaction alerts constitutes a relevant circumstance while determining the extent of liability, the same does not absolve the Respondent Bank of its primary obligation to exercise due care while acting upon electronic instructions involving substantial financial exposure. Consequently, this Authority is of the considered opinion that the Respondent Bank is liable for the loss suffered by the Complainant to the extent determined in the operative portion of this Order, having failed to establish compliance with the reasonable security practices and procedures expected under the Information Technology Act, 2000 and the applicable banking framework.

ORDER

- a) In view of the findings recorded hereinabove, the Respondent IDFC Bank Ltd. is held liable for failure to maintain reasonable security practices and procedures while processing the impugned electronic transactions under Section 43A of the Information Technology Act, 2000.
- b) Accordingly, the Respondent IDFC Bank Ltd. is hereby directed to pay the Complainant, M/s. Bharat Jyoti Impex, a sum of Rs.57,06,000/- (Rupees Fifty-Seven Lakhs Six Thousand Only) with interest at the rate of 12% per annum, calculated from the date of the unauthorized transactions until the date of actual realization.
- c) The aforesaid amount shall be paid to the Complainant within a period of 30 (Thirty) days from the date of this Order.

The order is passed on the date of digital signature, at Mantralaya, Mumbai.

Digitally signed by
Virendra Singh
Date: 11-08-2026
11:54:29

(Virendra Singh)

Secretary, Electronics, Information Technology &
Artificial Intelligence Department, Mantralaya,
Mumbai – 400 032.