BEFORE THE ADJUDICATING OFFICER,

SECRETARY
ELECTRONICS, INFORMATION TECHNOLOGY & ARTIFICAL INTELLIGENCE
MANTRALAYA, MUMBAI, MAHARASHTRA.

UNDER THE INFORMATION TECHNOLOGY ACT, 2000

IN

COMPLAINT CASE NUMBER 01 OF 2015

IN THE MATTER OF,

Mr. Jetho Sakhrani **)...Complainant**

Versus

Chief Manager, Punjab National Bank,
Andheri Branch, Mumbai. **)…Respondent**

Appearance:

Ms. Tejal Patel Advocate for the Complainant;

Ms. Puneet Bhasin Advocate for the Respondent;

[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 complainant, Mr. Jetho Sakhrani, a senior citizen and Non-Resident Indian, maintained an FCNR (Foreign Currency Non-Resident) account with Punjab National Bank since 2005, jointly with a family member. The Complainant had not availed of internet or phone banking facilities and relied exclusively on formal written correspondence with the bank.

2. In January 2013, the complainant discovered that his email account was compromised by an unknown hacker or impersonator, who fraudulently communicated with the Respondent bank and induced it to transfer funds from the complainant's FCNR account.

3. Acting solely upon email instructions, without proper verification or authentication, the Respondent bank effected an international wire transfer of USD 92,420 to an overseas account in Singapore.

4. The complainant alleges that the respondent failed to implement reasonable security practices and procedures as mandated under the Information Technology Act, 2000, thereby making it liable for compensation.

II. Chronology of Events:

1. The complainant opened and maintained his FCNR account with the respondent bank since 2005, with no prior incidents and no usage of electronic banking modes. On **28 December 2012**, the hacker/impersonator initiated fraudulent email communication with the bank, seeking details of the complainant's account and requesting fund transfer under false pretenses. On **01 January 2013 and 02 January 2013**, further emails along with a forged authorization letter were sent to the bank requesting wire transfer of funds to a Singapore account (as per *Exhibit-B* of complainant's documents).

2. On **03 January 2013**, the respondent bank acted upon the said emails and executed a SWIFT transfer of USD 92,420 to an account held in DBS Bank, Singapore, via Wells Fargo Bank (as per *Exhibit-E* of complainant's documents). Shortly thereafter, between 3 January and 5 January 2013, the complainant, upon noticing suspicious activity and email communications, immediately contacted the bank and clarified that he had not issued any such instructions and that his email account had been compromised.

3. Following this, on **08 January 2013**, a police complaint was lodged with the Singapore Police, and the respondent also registered a complaint with cyber-crime authorities in Mumbai on **11 January, 2013** (as per *Exhibit-F* of complainant's documents).

4. Despite initial assurances by the respondent bank on **27 February, 2013** that the matter would be resolved and funds would be recovered if no fault was found on the complainant's part, only a partial amount was frozen(as per *Exhibit-G*, point no. 4 of complainant's documents).

5. During the course of investigation, it was revealed that the accused, Tang Chew Yew, had been apprehended in Singapore and had pleaded guilty (as per *Exhibit-G, Page 3/3* of respondent's documents); however, a substantial portion of the transferred funds had already been withdrawn. On **20 August 2014**, an amount of SGD 42,787.04 (being a partial recovery of USD 34,327.93) was received, leaving a balance amount unrecovered.

6. Subsequently, on **29 August 2014**, the respondent bank informed the complainant that the matter stood concluded and denied liability for the remaining loss (as per *Exhibit-I* of complainant's documents).

7. Aggrieved by the Respondent's refusal to compensate and alleging gross negligence in handling sensitive financial instructions, the complainant filed the present complaint under the Information Technology Act, 2000 before the Adjudicating Officer.

III. Findings:

1. Reasonable opportunities were given to both parties to present their case and the matter was heard at length.

2. It is observed from the record that several material discrepancies and suspicious indicators ("red flags") were present prior to execution of the impugned transaction, including:
    - i. Incorrect spelling of the joint account holder's name;
    - ii. Signature mismatch with bank records;
    - iii. Sudden and urgent request for transfer of substantial funds;
    - iv. Sole reliance on email communication without corroboration;
    - v. Lack of prior pattern of such transactions by the Complainant.

3. Despite the presence of multiple red flags, the Respondent proceeded with the transaction without undertaking enhanced due diligence. Such conduct reflects recklessness and lack of prudence, which falls short of the standard of care expected from a banking institution.

4. The Respondent has contended to argue lack of updated contact details and inability to reach the Complainant. This contention is untenable. Banks are under a continuing obligation to maintain and periodically update Know Your Customer (KYC) records, ensuring a comprehensive 360° customer profile, including:

   i. Updated contact details
   ii. Alternative communication channels
   iii. Risk profiling of the customer

5. The Respondent bank has failed to demonstrate that any periodic KYC updating or verification exercise was undertaken. A bank cannot absolve itself of liability by pleading absence of contact details when such absence is itself a consequence of its own failure to maintain updated records.

6. There exists a **direct correlation between the Respondent's failure to act upon evident red flags and the resultant financial loss**. Had the Respondent exercised due diligence, the fraudulent transaction could have been prevented.

7. This Authority also acknowledges that customers are expected to exercise reasonable caution in safeguarding their email accounts and digital credentials. However, such responsibility does not dilute or override the higher standard of care imposed upon banks, particularly where systemic safeguards could have prevented the fraud. Thus, any contributory negligence on the part of the Complainant is minimal and does not dilute the higher standard of care imposed upon banks.

8. It is also necessary to mention here that customers not only deposit their funds and valuables with the banks for safe-keep but they repose a trust that their funds and valuables will remain safe. By failing to honor the trust reposed the bank has caused the complainant who also is a senior citizen, a financial and mental trauma.

9. **In light of the aforementioned finding in my considered view**, the bank has failed in its primary duty of keeping the funds of the complainant immune from any fraudulent activity despite a number of red flags. Accordingly, the following order is being pronounced-

ORDER

a. The bank is hereby ordered to refund the remaining amount of the defrauded funds i.e. USD 58,092.07 along with 12% interest to the complainant within a period of four weeks from the date of this order.
b. No order as to the costs.

The order is passed on 04th day of May, 2026, at Mantralaya, Mumbai and is digitally signed.

GOVERNMENT OF MAHARASHTRA
ADJUDICATING OFFICER
MUMBAI

Digitally signed by VIRENDRA SINGH
Date: 04-05-2026 18:06:26

(Virendra Singh)

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