

BEFORE THE ADJUDICATING OFFICER

SH. VIJAY KUMAR GAUTAM
PRINCIPAL SECRETARY, INFORMATION TECHNOLOGY,
GOVERNMENT OF MAHARASHTRA

Complaint No. 39 of 2015 dated 13th July, 2015

IN THE MATTER OF

Mr. Nirmalkumar Shankarrao AthawaleComplainant
Versus
Bank of India, Vaishali Nagar Branch, NagpurRespondent

Advocates:

1. For Complainant - Adv. Mahendra Bhaskar Limaye , Adv. Rajesh Tekale
2. For Respondent - Adv. Umesh G. Deshpande

JUDGEMENT

1. Brief Facts of the Case:

- 1.1 This proceeding emanates from the complaint filed by the complainant under Section 43 (a), (g), (h) and 43 A for Adjudication under Section 46 of the Information Technology Act, 2000. Following the basic principles of natural justice, reasonable and equitable opportunity of being heard was provided to both parties to present and defend their case. Following the completion of hearing and response of all concerned parties, conclusion has been arrived at and the judgment is being delivered herein.
- 1.2 From the complaint and documents enclosed with the complaint, written statement submitted by the Respondent, the admitted facts are that –
 - (a) The Complainant opened a Joint Savings Bank Account No. 877610110000176 (herein after referred to as the 'Said Account'),



jointly his wife, with Bank of India, Vaishali Nagar Br., Nagpur on 17.01.2015. The complainant's address & mobile number is registered with the bank. Internet Banking Facility was provided in this account by the Bank, as admitted by the respondent (Branch) in para 6 of its written statement, as "intricate part of associated with CID" without the explicit request of the customer/account holder.

- (b) The Complainant had a Sole Savings Bank Account No. 871810310000551 (herein after referred to as 'Other Account'), only in his name, with Customer ID (CID) 900634551 in Kamptee Branch of Bank of India opened on 07.01.2015 and closed subsequently on 21.04.2015. On the request of the account holder (complainant in the present case), Internet Banking Facility was provided in this account.
- (c) The Complainant received information from Bank of India, Vaishali Nagar Br., Nagpur on 27.06.2015 that some financial transactions debiting Rs. 3,00,100/- from his Joint Savings Bank Account No. 877610110000176 occurred using Net Banking Facility.
- (d) The complainant submitted written complaint to the bank on 29.06.2015 and filed FIR No. 233 with Police Station, Paachpaavali on 4/7/2015.
- (e) The complainant was informed about beneficiaries of the said fraudulent transaction by the bank and Rs. 50,100/- were credited to his account on 01.07.2015 by freezing the beneficiaries' account by the bank. The amount Rs. 250000/- could not be recovered till date as it was withdrawn from respective accounts both belonging to Bank of India.

1.3 The contention of the complainant are:

- (a) That the account holders (the complainant and his wife) never submitted any request for availing internet banking facility in the said account.



- (b) That the internet banking facility is an additional service offered by the banks and can only be provided when a customer specifically applies, as he had done for the other account, to avail such facility and, therefore, bank has not only gravely erred in activating internet banking facility in the said account without the request of account holder but has committed serious security breach by not intimating the complainant about such activation.
- (c) That the gravity of the error is multiplied by the fact that the complainant never received any SMS, which is the standard process for any internet bank facility transaction, about such transaction despite his mobile number being registered with the bank.
- (d) That the bank has compromised with the reasonable security practices by erring to import CID from other account and providing the not-asked-for facility in the said account and making the complainant/account holder vulnerable to such fraud by not intimating him about such activation and, further, by not linking his mobile number with the said account for intimation of any consequent transaction in the said account.
- (e) That the argument of linking the CID from the other account does not hold any ground because the constitution of these two accounts make them different accounts and, therefore, establish two separate identities requiring two different CIDs.
- (f) That in view of above, the bank has definitely been guilty of contravention of Section 43 (a), (g), (h) and 43A leading to irreversible financial loss to the complainant and, therefore, the claim of damages of Rs. 3,50,000/- (Rs. 2,50,000/- being irrelevant transactions charged to the customer's account by bank , Rs. 80000/- against the legal charges and Rs. 20000/- for compensation for mental harassment) be awarded in his favour.



1.4 In the reply submitted through written statement and during the oral argument before me, the respondent contends that –

- (a) The CID code is universal in nature and the CID No. 900634551, originally generated at Kamptee branch of Bank of India for the other account, was operated to open the said account at Vaishali Nagar Branch. It is a banking practice to use the CID code of a customer profile to be used universally.
- (b) The CID of the other account was already provided with internet banking facility.
- (c) The internet banking facility is the intricate part of associated with CID.
- (d) The said account opened on 17.01.2015 was with pre-existing internet facility.
- (e) The bank has acted promptly after getting the information of the fraud transaction by the IT Dept., Bank of India, Nagpur and frozen the beneficiaries accounts after reversing the entry amounting to Rs. 50,100/-.
- (f) The complainant has nowhere mentioned how the third party got an access to his bank account having a facility of internet banking. The provider of the internet mobile services played the vital role in causing the access to the complainant's account to the criminals committing the cyber-crimes. The bank was without the knowledge of the cyber criminals getting access to the complainant's account, as the said access is provided due to fraudulent provision of Mobile SIM Card/connectivity by the mobile service providers. The complainant has failed to make the mobile service provider as the chief institute responsible to cause the fraudulent transfer with intention to paint the Respondent as the culprit.



- (g) The complainant has full confidence in the Respondent Bank as he has not shifted his account to any other Bank and continuing his banking transactions using the same branch.
 - (h) The Bank has neither violated security practices as mentioned in Section 43 of I.T. Act or any other clause of I.T. Act or C.P.C/I.P.C.
 - (i) In view of above, the complaint may be rejected with cost.
- 1.5 In his written re-joinder, the complainant, in addition to reasserting his contention put earlier, submits that –
- (a) The said account in Respondent bank is kept operational for the convenience of the bank so that if bank's fraud investigation unit finds the destinations of money, the same can be reverted back in complainant's account.
 - (b) There is definite contravention of provisions of Section 43A of I.T. Act which specifically provides relief for failure to protect data which has happened in this case by respondent Bank.
- 1.6 On the closure of the arguments by both the parties and after waiting for considerable time to get the report of investigation by the Police, it has been to decide the matter on the merit of the arguments put forth by both the parties for the sake of justice within the limited framework of the IT Act 2000.
- 1.7 On consideration of the detailed arguments, oral as well as written, put forward by both the parties, and in view of the provisions of the IT Act 2000, the key issues and findings are recorded as follows:-

Issue No. 1: Whether the Said Account and the Other Account can be treated as accounts with same customer profile and, therefore, same customer ID (CID) could be allotted to both accounts?

Findings: NO. The bank has drawn erroneous conclusion of the 'Universality



of CID code of a customer profile'. The present case is concrete example where the CID code assigned to the complainant in his other account would, at best, contain the individual profile details of the complainant but not of his wife who is a joint account holder in the said account. The contention of the respondent can be accepted limited to confirming the customer profile of the complainant through a CID created earlier but cannot be accepted where a different account with two joint holders and with operational instructions of 'Either' or 'Survivor' is being opened. The copy of the passbook for the said account submitted with the complaint, incidentally, mentions a different CID 152945369 and, therefore, indirectly corroborates that these two accounts were treated differently leading to assignment of different CID to the said account at the time opening as recorded in the passbook. No light has been thrown by respondent that by which established procedure known to account holders, the CID of a single account holder from the other account was linked, for operational purposes, with the said account held jointly by two different account holders. Even if the contention of the bank is taken for consideration for argument sake, the question is which CID would have been given to the said account had the complainant and his co-account holder had different CIDs from their previous single accounts in some other branch of the same bank? What steps bank would have taken if one CID from previous account was linked with internet bank facility and the other CID was not? It is a known fact that compliance with Know Your Customer (KYC) norms is mandatory for each of the account holders and for the sake of reducing paper work banks may be finding the existing CID useful in importing personal profile of a particular CID holder and tracking his/her personal profile across multiple accounts. However, extending the logic to treating an account with single account holder (in this case the other account) to be same as an account with multiple account holders (in this case the said account) is absurd. Therefore, respondent's argument based on the universal nature of CID code and to further act to provide internet banking facility in the said account does not hold ground at all.



Issue No. 2: Whether services like Internet Mobile Banking can be provided without the request of the account holder customer and, in the event of such one sided decision taken by the bank, whether no intimation to the customer about activation of such facility is required to be given?

Findings: NO. The manner and mode of operation of any bank account is the sole prerogative of the customer/account holder(s) subject to the capability of the bank to cater to such need/requirement of the customer. It is the responsibility of the bank to offer such innovative financial services to the customers and, at best, pursue them to avail the services depending on their personal and business requirements. Further, Internet Mobile Banking, a Fintech driven service combining the strengths of internet, data analytics and artificial intelligence, has been adopted by the banks to remain competitive in today's financial services industry driven by the educated and demanding customers' expectations. Since such services require customer preference or comfort level with use of technology as well as availability of requisite resource such as internet connectivity, enabled hardware (handheld or otherwise), no such service can be thrust upon the customer without his request or at least consent. It is beyond explanation that what purpose a facility would serve if the customer, for whose comfort/ease, presumably, such facility is activated, is not even aware of it. The contention of the respondent that the internet banking facility, being 'intricate part of associated with CID', can be automatically activated in any other account where the customer holding the CID is co-account holder with other(s) without the consent of all the account holders cannot be accepted. Further, such practice definitely exposes the financial transaction processes in such accounts to the security risks as has happened in this case. The contention of the respondent regarding the birth of the said account with congenital ascription of internet banking facility presents a farcical logic in the absence of any published policy of the bank regarding new opening of accounts with pre-



existing internet banking facility. Therefore, there is no iota of doubt that bank has committed serious mistake in providing internet banking facility to the said account of the complainant without his request and has immensely multiplied its mistake by not even intimating the account holders of the said account regarding such facility being activated.

Issue No. 3: Whether the action of activating internet banking facility in the said account without the request of the account holders, neither seeking consent nor giving any intimation to them about such facility and not providing alerts about any financial transaction in the said account on the registered mobile number of the complainant, the bank, which owns, controls and operates the customers' sensitive personal data and information, has been negligent in implementing and maintaining reasonable security practices and procedures and, thereby, creating a conducive environment for person(s) with malafide intention to cause wrongful loss to the complainant and, consequently, wrongful gain to such mischievous person(s)?

Finding: YES. It is a fact that the bank owns controls and operates the customers' personal data, financial transaction processes and procedures and financial transaction data. Further, there is no doubt that these data constitute information on financial transactions, financial health etc. of the customers and, therefore, extremely sensitive in nature and cannot be shared or allowed to be shared, by any act of omission and commission, unless as required by the customers or under due process of law. In the light of findings in Issues Nos. 1 & 2 above, it is established that the bank has been immensely negligent in – Firstly, treating a single account on par with a joint account and, therefore, linking the CID of the other account with the said account; Secondly, activating internet banking facility in the said account without the request or the consent of the account holders; and Thirdly, not intimating the account holders about activation of such facility in the new said account which was completely different in its nature and scope of



operational instructions. As mentioned in the findings of Issue No.1 above, retail banking being the most profitable segment of conventional banking (Citigroup 2016), Fintech driven products and services combining the strengths of internet, data analytics and artificial intelligence, has been extensively adopted by the banks to remain competitive in today's financial services industry driven by the educated and demanding customers' expectations. According to Prof. Peter Tufano, Dean of Said Business School, Oxford University, key emphasis areas for the financial service industry adopting fintech solutions are consumer experience and expectation with regards to transparency, convenience, simplicity, security and effectiveness. As the use of internet continues to grow and evolve, the vast amount of data about individuals are progressively put to data analytics and Artificial Intelligence is used to link multiple data sets lying across multiple locations, the measures available to protect personal data by entities (the bank in this case) owning, controlling and processing/operating such data has to become the key area of focus. Cyber security measures, consequent standard operating procedures and effective change management strategies, therefore, inevitably become the integral part of the Fintech Eco-System adopted by the financial services industry. It is the responsibility of the banks who want to be competitive, commercially profitable and customer friendly by adoption of fintech innovation such as mobile banking, internet banking, etc. to ensure that a pro-active and predictive cyber security framework is established with contemporary technological measures, consequent standard operating procedures and requisite change management strategy across the organization. Unfortunately, as is evident form the facts and findings of this case that while the bank has adopted technological measures to introduce internet banking facility, it has miserably missed out on the adoption of requisite operating procedures to introduce transparency, security and effectiveness. The contention of the respondent on universality of CID, automatic activation of the internet banking facility, perception on account being opened with pre-existing internet banking facility, no consent from or



intimation to account holders etc. establish that cyber security measures have not been given priority by the bank while adopting fintech innovation to become cost-effective and, thereby, profitable. It is further surprising to note that while the account holders, for whose convenience internet banking facility was presumably activated in the said account, were kept unaware of such facility, some other persons having accounts in the same bank became aware of the activation of such facility in the said account and could successfully cause 'wrongful loss' to the complainant and, consequently, 'wrongful gain' to themselves. A gross failure by the bank in implementing reasonable security practice has occurred when it failed in intimating the complainant about such transactions by SMS to the mobile number of the complainant registered with the said account. Intimation by SMS is a well-known practice followed by banks, for long now, in intimating all financial transactions whether conventional or digital to the account holders. While the respondent has dared to submit absurd reasons of genetics for automatic activation of internet banking facility by keeping the complainant in complete dark, it has completely forgotten to follow even the conventional banking practice of intimating the account holder immediately about the financial transactions in the said account and, consequently, making him completely helpless in taking any appropriate action in time. This gross negligence in implementation and maintenance of even basic security measures and practices by the bank has definitely made the complainant completely vulnerable causing irreversible 'wrongful loss' to him. It is intriguing to note that the bank has informed about such doubtful transactions to the complainant on 27.06.2017 on information from the IT department of the bank at Nagpur while the transactions occurred on 22.06.2017. No explanation has been furnished on the cause of this certain action by the IT department of the bank. It raises doubt about the whole cyber security framework of the bank which, far from being pro-active or predictive, appears to be in the dormant stage leaving an average customer, with little or no knowledge and resources to appreciate and handle such complexities,



completely vulnerable. It is evident that such gross negligence has not only caused wrongful loss but immense mental agony to an average customer, with limited resources, to go for litigation against mighty bank spending millions on adoption of technology.

- 1.8 Conclusion: In view of the findings on all the relevant issues as above, I have come to the conclusion that there is enough evidence on record to establish that the action of activating internet banking facility in the said account without the request of the account holders, by neither seeking consent nor giving any intimation to them about such facility and by not providing alerts on the registered mobile number of the complainant about the malicious financial transactions in the said account, the bank, which owns, controls and operates the customers' sensitive personal data and information, has been gravely negligent in implementing and maintaining reasonable security practices and procedures and, thereby, creating a conducive environment for person(s) with malafide intention to cause wrongful loss to the complainant and, consequently, wrongful gain to such mischievous person(s) and, therefore, makes the respondent bank liable for violation of Section 43A of the IT Act 2000 which reads as –

"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person affected."


ORDER

In the light of above, under the powers conferred on me under Section 46 of the Information Technology Act, 2000, I pass the order that the respondents shall pay by way of compensation to the complainant a total amount of Rs. 3,50,000/- (Rupees Three Lacs Fifty Thousand Only) to cover the wrongful loss caused, legal costs and for



the mental agony suffered by him within a month of this order, failing which a compound interest of 12% compounded monthly will be chargeable.

Order passed on this day of 9th November, 2017 at Mumbai.


(Vijay Kumar Gautam)

Principal Secretary, Information Technology,
Government of Maharashtra,
Mantralaya, Mumbai-32