IN THE OFFICE OF THE ADJUDICATING OFFICER OF JUDICATURE AT CHENNAI

Thiru PWC Davidar, IAS, Adjudicating Officer
Secretary to Government, Information Technology Department,
Government of Tamil Nadu

CIVIL JURISDICTION
PETITION NO.2462 OF 2008

Dated : 12th April 2010

Shri Umashankar Sivasubramanian .. **Petitioner**

Versus

1) The Branch Manager
ICICI Bank
Tuticorin Branch
Door No.19, V.E. Road,
Tuticorin-628002
Tamil Nadu

2) The Manager,
ICICI Bank
Fort Branch
Navsari Building
240, D.N. Road,Fort
Mumbai-400001

3) Shri Murali Nambiar
AGM, Head Information Security
ICICI Bank Limited
ICICI Bank Towers
Bandra Kurla Complex
Mumbai-400 051

4)Shri KV Kamat
Managing Director
ICICI Bank Limited
ICICI Bank Towers
Bandra Kurla Complex
Mumbai - 400 051

5) M/s Uday Enterprises(through ICICI Bank),
Current A/c Holder No.623505378469
C/o Manager, ICICI Bank,
Navsari Building
240, D.N. Road, Fort
Mumbai-400 001 .. **Respondent**
ICICI Bank, Mumbai

Mr. Na Vijayashankar, Techno Legal consultant and **Mr. C. Sivasubramanian** for the Petitioner.

Mr. R. PremKumar, Senior Manager-Legal, and **Mr. Gopi Narayanan**, ICICI Bank, Chennai for Respondent No.1 to 3.

Judgment

1. This is the proceedings of an application filed by the petitioner for Adjudication under section 43 read along with section 46 of the Information Technology Act 2000. In a follow up to the IT Act of 2000, under powers conferred by the Act, the Government of India have issued IT Rules (certifying authorities) 2000, Cyber Regulations Appellate Tribunal Rules, 2000 and other rules inclusive of Notification No.GSR 220(E) dated 17.3.2003 and 240(E) dated 25.3.2003 by which the Secretary to Information Technology of each state is notified as the 'Adjudication Officer' under the IT Act 2000. Consequent on the notification issued by the Government of India, the State Government has appointed the Secretary to Government, Information Technology Department as the Adjudicating Officer for the State. Further, section 46 sub section (5) of the IT Act also states that every Adjudicating Officer shall have the powers of the civil court and all proceedings before the Adjudicating Officer shall be deemed to be judicial proceedings within the meaning of section 193 and 228 of the Indian Penal Code. In keeping with the basic principles of justice, detailed hearings were held in which both parties i.e., the petitioner and the respondent were provided equal and adequate opportunities to present and defend their case. Following the completion of hearing and submission of affidavits and counter-affidavits, the conclusion is being arrived at and the judgment being delivered herein.

Petitioner

2. The petitioner (complainant) is a non-resident Indian and is employed as a Process Engineer, Dept: SUFEMS, ZAKUM Development Company in Abu Dhabi and is currently residing in Abu Dhabi. His permanent residential address

is at 4/125/2 State Bank Colony North, Tuticorin – 628002. The petitioner maintains a savings bank account (NRE) with ICICI Bank, V.E. Road, Tuticorin and the bank account number is 613901200505. The Bank has activated an Internet Banking facility for the account. Every month, the ICICI Bank NRI Services Team would send a statement of account to the petitioner of this case from an email id, the URL of which is customercare@icicibank.com . At the end of August 2007, the balance in the petitioner's account was Rs.6,20,846 and on 4th September the ICICI Bank credited an interest component of Rs.25,200 which then increased the petitioner's credit balance to Rs.6,46,046. The entire incident begins when the customer had received a security update from customercare@icicibank.com for updation and assuming it to be a routine mail from the ICICI Bank that had sent similar mails earlier, the customer had complied with the request consequent to which he was shocked to find that his account had been debited to the extent already mentioned.

3. According to the petitioner, he received a telephone call from ICICI Bank Mumbai on September 7th , 2007 when a representative from ICICI Bank, Mumbai telephoned at 1800 hours (UAE time) and requested for confirmation whether money transfer from the petitioners account had been made to 'Uday Enterprises', Mumbai through Internet banking on 6th and 7th September 2007. The petitioner denied any transfer being made as suggested by the Mumbai branch. The ICICI Branch accordingly instructed the petitioner that a complaint be filed within 24 hours to Customer Care, ICICI Bank Mumbai which was done by the petitioner and a reference number given as SR37195467. Following this, the petitioner faxed and emailed a complaint to the ICICI Bank Tuticorin and the NRI services center, Mumbai.

4. Following this, an email was received from the Customer Service Quality department of the International Banking Division of ICICI Bank that the matter was being investigated and that within a month's time they would revert with a resolution. The petitioner then receives a mail on October 20, 2007 (43 days after the loss of money from his account) from one Mr.Shankar representing the respondent bank on the immediate results of the investigation. This mail from ICICI was sent by a personal email id on a Gmail account and not on the official ICICI email id. The details of investigation as reported in the mail indicate the following: a) that the incident appears to be a case of Actual Infinity Phishing Fraud b) that the petitioner's account has been debited to the tune of Rs.6,46,000 and that the funds were transferred to ICICI A/c no: 623505378469 which belonged to Uday Enterprises c) that Uday enterprises was a current account and a partnership account with ICICI Mumbai and d) that the account was in debit balance since 23-04-2007 and e) that an amount of Rs.4,60,000 was withdrawn by Self Cheque across the counter from the Uday Enterprises account. The mail goes on to indicate that the mail is marked for CCTV clippings

and the address of the beneficiary is indicated. f) The report further indicates that the address of Uday enterprises was visited and the door was locked and the residents there indicated that Uday Enterprises had shifted two years earlier. Further verification reveals to the Bank that the firm is a proprietorship firm and the proprietor's name is Mohd Zulfqar Hasim Khan apart from the documents submitted for proof to the bank and that the firm had been in existence at the same address until two years ago. The investigation report comments that as the immediate case refers to a phishing case, the blame of negligence lies with the customer and that the customer would need to file the FIR.

The observations in the investigation report states that the customer (presumably referred to as cm in the report) should file the FIR and then the case can be closed. An observation is also made that the 'beneficiary' (namely Uday enterprises) account has still a balance of Rs.1, 50,171/- and which needs to reversed. This amount of Rs.1,50,171/- was subsequently reversed on 17th July 2008 into the petitioner's customer's account. There is also a reference in the report that the KYC (Know your Customer) is positive at the time of opening of the account (Uday Enterprises) but this has not been detailed. The final remark of the ICICI Bank's report is that the case is closed and that the beneficiary is untraceable .

5. The petitioner filed a complaint before the Superintendent of Police in Tuticorin detailing all the events and indicated the possibility of the Bank or some of its staff being behind the fraud. The petitioner requests the police to 'initiate action against the ICICI Bank and retrieve the money. This petition was subsequently transferred to the Cyber Crime Police Station at Chennai. On the 6th February, 2008, the petitioner lodged a fresh complaint with the Cyber Crime Cell, CCB at Chennai.

6. Finally, the petitioner has concluded in his application that ICICI is primarily responsible for the loss and that Uday Enterprises may be a benami of the bank or any of its staff members. He has alleged that due diligence has not been made by the bank in the entire case and in the case of Uday Enterprises particularly when the account had actually been in overdraft and suddenly to have been into a high transaction. Further, he has stated that such a large transaction by way of a self-cheque over the counter without adhering to banking norms is indicative of negligence on the part of the Bank. The immediate adjustment of the overdraft of Uday Enterprises by the money so transferred has also been questioned. The failure of the Bank to file a criminal complaint on the matter in Mumbai even after the fraud has come to light, failure to retain a record of the CCTV clippings, failure of the Bank to adequately adhere to the KYC (Know your customer) norms, failure to part with the IP addresses immediately after the incident that had led to the fraudulent transfer and lack of maintenance of record of the same in violation of RBI instructions, failure to use digital signatures in official

communication, lack of adequate controls by the Bank to ensure information security, that Sections 11, 66, 43, 85 of the IT Act have to be considered in the light of all the facts and they have a bearing on the gross negligence of the Bank in causing loss to the petitioner and all of these together have to be considered in dealing with the petition made by the petitioner under Section 43 and Section 46 of the IT Act of 2000.

7. The petitioner in the course of the hearing filed an additional reply to the initial counter affidavit filed by ICICI bank. He has stated in addition to his earlier statement that there is due justification in having approached the adjudicator as he is the main avenue for redressal of the issue on account of the fraud propitiated on him and it being within the purview of the Information Technology Act of 2000. Approaching the banking ombudsman was for the redressal of the customer complaint and not replacement of any other remedy and the complaint at Tuticorin Police Station was on account of this being a cognizable offence. The cyber crime Police Station registering an FIR under Section 66 of IT Act 2000 of the initial investigation confirmed this. In this the petitioner has expressed his disappointment on the failure of the respondent bank to file a complaint in Mumbai even after being aware that the final beneficiary of this IT fraud was also their customer. Also, the petitioner has recorded his opinion with regard to the jurisdictional relevance of the adjudicator and the powers therein to try this case according to the IT Act, 2000.

Respondent

8. In response to the complaint filed by the petitioner, the respondent submitted the following:
That the respondent bank provides net banking services to customers among other services and that the internet banking services includes transfer of funds, respondent enquiries about details in the transactions of his account, statement of account etc. Accordingly, at the time of opening of the account by a customer, the customer agrees to the conditions imposed by the bank and unconditionally undertakes to have the user ID provided by ICICI bank changed and ensured that the same is kept confidential and not to let any unauthorized person to have access to the same and neither ICICI bank nor its affiliates shall be liable for any unauthorized transactions occurring through internet banking and the user then fully indemnifies and holds ICICI bank harmless against any actions, suit proceeded against it.

9. According to the respondent, the complainant has negligently disclosed the confidential information such as password and thereby had fallen prey to a phishing fraud. According to the bank, customers of the bank are fully apprised on security aspects of internet banking through channels such as monthly/quarterly statement, posters located at ATMs and branches,

information through the website of the bank at www.icicibank.com to safeguard their own interest.

10. The ICICI bank as respondent has also affirmed that it has adopted information security policies and guidelines for the bank in order to safeguard the interest of its customers. As part of this commitment, the respondent bank had cautioned its customers through the bank's web page on "fraudulent e-mails requesting online banking security details" and information on methods used in phishing. Further, that tips to protect the customers from phishing were also available on its web site which included a statement that ICICI bank would never send e-mails asking for confidential information. Also, the bank had appraised the customers in general to treat all unsolicited e-mails with caution and never to click on links in e-mails to enter confidential information. In addition to this, the bank has informed the customers that it will not be liable for any loss arising from sharing mobile user Ids / passwords/pin numbers with anyone by customers.

11. The respondent bank also denied the charge that they had not complied with Know your Customer (KYC) requirements issued by RBI. According to the Bank, the current account of Uday enterprises that had benefitted from this illegal transaction had been verified for address and identity. According to the respondent Bank, the customer had operated the account in a satisfactory manner from 2005. The KYC documents relied upon were the telephone bill, pan card and sales tax certificates issued by the Maharashtra Government. According to the respondent, the provisions of the Negotiable Instrument Act and AML requirements have not been violated.

12. According to the respondent, they have conducted an investigation through the risk containment unit of the bank. Also, as the phishing e-mails are sent using forged e-mails and as it does not originate from the ICICI bank e-mail server, the bank has no control over the origination of e-mails.

13. Further, the respondent bank submitted that Uday enterprises owed a sum of Rs.35, 000/- to the respondent bank towards credit facility and that as soon as the funds flowed into that account, it was duly adjusted against it. The bank states that it is entirely the complainant's negligence in overlooking the security guidelines and alerts given by it which has resulted in the present loss to the complainant. The respondent bank also states that it has given a credit of Rs.1, 50,171/- at the request of the complainant which was available in the account of Uday enterprises. Further, the bank submitted that the CCTV clipping will be available only for a period of one month. The respondent bank also denied that they use password as the only source for authentication and have other sources of authentication such as mobile alerts, SMS confirmation etc.

14. The Respondent bank states that the adjudication officer in the current case has no apparent jurisdiction and that the complaint cannot be seen as within the purview of the IT Act. The respondent is of the opinion that as a criminal complaint had been filed, it was now the responsibility of the police to conduct a criminal investigation and that the bank had nothing to prove in the matter. The respondent bank also opines that the subject matter of this case cannot be brought within the provisions of the IT Act of 2000

Judgment

15. The immediate task at hand is to first establish whether or not this petition is within the purview of the IT Act of 2000 as insisted upon by the petitioner. The scope of jurisdiction will determine then whether the petitioner's complaint is to be deliberated upon and whether a conclusion has to be arrived at by this adjudication officer. The petitioner has filed the request for adjudication under section 43 read with section 46 of the Information Technology Act 2000 and as per the guidelines contained under notification No. GSR 220(E) dated 17 March 2003 and GSR 240(E) dated 25 March 2003 of Ministry of Communications and Information Technology, GOI. The petitioner, in particular has invoked section 85 of the IT Act on the lack of due diligence by the respondent in preventing the act that falls within the scope of Section 43 of the IT Act and a few other relevant sections of law. Also, that the said contravention has been carried out with the knowledge of the respondent bank which is a banking company. In particular, section 85(2) dwells on such contravention having taken place with the connivance of or attributable to any neglect of the company or of any member of the company. Considering the immediate defense of the respondent bank in questioning the jurisdiction of this office, it is essential to determine whether the adjudicating officer has jurisdiction over this case in particular.

16. Section 43 of the IT Act covers the scope of the section that can invite penalty and the relevant parts of the section to this case read as follows. Section 43: 'If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, -

43(a) Accesses or secures access to such computer, computer system or computer network;

43(b) Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

43(d) Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer

network;
43(f) Denies or causes disruption of any computer, computer system or computer network by any means;
43(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder'.

17. Section 85 (1) of the IT Act that deals with offences by companies extends the above section further and states as follows: 'where a person committing a contravention of any of the provisions of this Act or any rule, direction or order made there under is a company, every person who at the time the contravention was committed was in charge of and was responsible, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly: Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

Section 85 (2) states further notwithstanding anything contained in sub-section (1) where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

18. On an analysis of these two sections and the petitioner's application in this case, the following facts are noticed. Section 43 read with section 85 of the Act clearly highlight that this case falls within the jurisdiction of this office as the offence made out is within the purview of the IT Act of 2000. The petitioner has placed his trust in the services offered by the Respondent Bank (a Banking company) in providing a secure environment for his finances and has operated an account in the respondent Bank Branch. In furtherance of this trust, and reliability offered by the respondent bank in providing secure transactions over the Internet, and due to fact that he was working in another country several thousand miles away, the petitioner has extended his trust into operating his Bank account in the Respondent's Bank Branch in Tuticorin through the Internet. In this process, due to a transaction that he assumed as genuine, he has suffered financial loss which he would not have suffered had he stayed away from operating an Internet Account. A prima facie case of the matter attracting the relevant provisions of the Information Technology Act is made out.

As a result of the incident, there has been unauthorized access to the petitioner's account in the respondent account, loss of data and account information of the petitioner, damage to electronic information of the petitioner which resulted in financial loss, denial of access to his account due to operation of the same without due authorization from him, and a complete loss of trust on the respondent bank and the belief that such a financial loss would not have occurred if the respondent had not exercised due diligence in the matter to prevent such a contravention. Additionally, that such a loss would not have occurred without the connivance or neglect on the part of the respondent bank. The petitioner has filed his complaint against the respondent bank on the above grounds, all of which falls squarely within the scope of Section 43 read with Section 85 of the IT Act. The adjudicating officer is then faced with the question as to whether the petitioner has exercised all due diligence to prevent the financial loss to the petitioner that has occurred through the Internet Banking system installed by the Respondent Bank. Also, the adjudicating officer is faced with the situation of assessing whether the petitioner is entirely liable for the situation that he is in and whether he is justified or otherwise in the content of his petition. Thus, this case falls within the scope of the adjudicating officer in the light of the above. Having stated that this case is entirely relevant to this office and well within the scope of jurisdiction of the adjudicating officer under the relevant provisions of the IT Act, it is now appropriate to conclusively assess in the light of all the facts provided herein as to which one of the two parties stand is justified i.e., the petitioner or the respondent.

19. To begin with, the petitioner has been regularly receiving account statements from the respondent bank which were sent by Internet through email. This activity of the bank in sending such mails has taken place in a routine manner. As and when these account statements arrived by email, from a particular email id which hitherto had been used by the bank, the petitioner assumed that this was from the respondent bank. The bank did not take any particular step to distinguish between emails that had originated from their office as against emails that had arrived from elsewhere. The respondent bank in defense of their actions has drawn attention to their formal list of instructions that would go out to any customer and that are also posted on the bank's website. The respondent has taken shelter behind the routine instructions on phishing as posted in the website and has stayed away from taking adequate steps and precautions to prevent contravention of unauthorized access which would have benefitted the customer. The instructions posted are of a routine nature and do not help the customer to distinguish an email that has arrived from the respondent bank as against one which is from elsewhere. Authentication and validation is a key element in any transaction and more so when financial transactions are the mainstay of the activity. In the context of the Internet, this acquires paramount importance. A

customer should know beyond any reasonable doubt that a communication received from the bank is authentic and has been validated by the sender bank as a mail that has originated from their servers. This precaution has not been taken by the respondent bank. In other words, there was no manner by which this customer could identify a mail as being from the respondent bank. A facile and simple method would have been for the respondent bank to acquire a digital signature for the officer responsible for communicating with customers and thereby provide one layer in authentication of such mails. The respondent bank could have also incorporated another layer of authentication to help a customer distinguish and identify when an email is genuinely from the bank and when it is not. There appears to be no effort of that nature by the respondent bank. Even in the matter of drawal of money from the account, additional layers of safeguards, automatic SMS alerts to the customer when money is drawn from his account etc, could have contained the damage to the petitioner customer. Due diligence in the matter has not been exercised by the bank which could have prevented the extent of fraud on the petitioner customer. The systems in the respondent bank do not appear to be streamlined as can be seen in para 4 of this judgement wherein the official report of the bank is sent by the investigating officer and the communication has been sent by a gmail account and not the official id of the respondent bank. There is apparently no standard communication ethic or code for the respondent bank's staff with customers.

20. Secondly, the chain of events after the unauthorized access by a third party on the petitioner's account leaves much to be desired and reflects very poorly on the respondent bank's systems and procedures in the event of a customer facing a situation of this kind related to an Internet account that has been accessed in an unauthorized manner. The customer was requested to file a complaint with customer care in the same bank and following this a 'final report' was given. After such a major fraud having taken place in the bank premises the branch submitted itself to an internal enquiry only to give a final report. However, no action was initiated by the respondent Bank Branch either from Tuticorin (where the petitioner had his base account) or Mumbai (where the person who gained unauthorized access was an account holder) in filing of a criminal complaint even after it was clear that the customer who was registered in its Mumbai branch had fraudulently acted against another fellow customer in a different branch of the same bank while utilizing the Information technology vehicle that had been built, supported and maintained by the respondent bank. The respondent bank has appeared to function in a manner that would indicate that it has 'washed its hands off the customer'. This is further compounded by the fact that the money removed from the petitioner's account has been handed over across the counter in a cash transaction to the perpetrator of the fraud, also a customer, who by the respondent's own admission had a debit balance. A great degree of indifference or systemic failure is evident for the respondent's officials

to refrain from carrying out even the minimum tasks required in such circumstances in helping a customer secure justice. It is possible to even assume a certain degree of complicity or indifference at the level of the respondent bank branch to the customer's plight.

21. Thirdly, para 3 of this judgment refers to a telephone call from ICICI Bank, Mumbai at 1800 hours (UAE time) on September 7th, 2007 to the petitioner who was then at Abu Dhabi. The telephone call requested for a confirmation as to whether a money transfer had been done to Uday enterprises in Mumbai. This appears to be strange as several thousand transactions from Account to Account take place on any particular day in a bank and it is not possible for any bank to keep track of every transaction of their customer. So it is found to be rather strange that such a call was even made. The respondent bank also was not forthcoming as to how it had suddenly felt that a telephone call would need to be given to the petitioner customer from its Mumbai based office with nothing systemic in place as to provide an alert. Without an automatically generated email alert or SMS alert being given even to the petitioner customer, a telephonic call to the customer leaves room for doubt in the manner of reaction from the ICICI Bank.

22. Fourthly, the Banking Codes and Standards Board of India which has set the minimum standards for banking practices with customers to be followed has incorporated in its model code that clearly implies that a bank may wish to investigate transactions and that police involvement and customer's involvement are anticipated in such a situation. Therefore, the response of the respondent Bank in choosing not to retain the CCTV clippings of the Mumbai Branch is rather strange and defies understanding. The Mumbai branch of the respondent had recorded by way of CCTV a video clipping that contained images of the individuals who had defrauded the petitioner. It is difficult to understand why the CCTV clippings of that day were not retained by the bank so as to assist in detecting the culprits involved. The very purpose of the CCTV being installed is seen to be defeated. Apart from the CCTV clippings not being retained, the respondent bank made no effort to involve the police in its investigation and follow up on the incident. As mentioned earlier, this needs to be seen in the light of the fact that the perpetrator of the fraud was a customer of the respondent Bank and this by the Bank's own admission.

23. Fifthly, the respondent bank is governed by the instructions and directives of the Reserve Bank of India (RBI). Master Circulars have been issued by the RBI which are unambiguous and categorical and which are expected to be scrupulously followed by all banks. Some of the instructions/directives which are oriented to the responsibilities of the bank as against a customer and those which have a direct bearing with customer relationships in Master circulars and which appear

to be violated are mentioned below. It is important to note that these instructions/directives hold good for all customers being serviced 'over the counter' or 'over the Internet'.

On Internet Banking in India certain Guidelines have been issued by RBI in DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01 on June 14, 2001. Certain relevant clauses are highlighted herein:

I. Technology and Security Standards:

The banks should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies. They should educate their security personnel and also the end-users on a continuous basis. (Para 6.4.7, 6.4.11, 6.4.12)

II. Legal Issues:

a) Considering the legal position prevalent, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about integrity and reputation of the prospective customer. Therefore, even though request for opening account can be accepted over Internet, accounts should be opened only after proper introduction and physical verification of the identity of the customer. (Para 7.2.1)

b) The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. Currently, the rights and liabilities of customers availing of Internet banking services are being determined by bilateral agreements between the banks and customers. Considering the banking practice and rights enjoyed by customers in traditional banking, banks' liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be assessed and banks providing Internet banking should insure themselves against such risks. (Para 7.11.1)

III. i) In the Master Circular on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act, (PMLA),2002 -also published on the RBI website at http://rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?Id=4354&Mode=0 of which the objective reads as follows: 'The objective of KYC/AML/CFT guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better which in turn helps them manage their risks prudently.

ii) Clause 2.5 reads Accounts of companies and firms ii) Banks need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Banks should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management.

iii) Clause 2.7 on Monitoring of Transactions reads as 'Ongoing monitoring is an essential element of effective KYC procedures. Banks can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. Banks should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Banks may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the bank. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts have to be subjected to intensified monitoring. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. Banks should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorization of customers should be carried out at a periodicity of not less than once in six months.

If these minimum requirements as had been directed by the Reserve Bank had been observed in the bank, the request of a customer who involves himself in an unauthorized, fraudulent cash transaction and benefiting from cash across the counter while having an overdrawn account for a period of time would have been detected and prevented easily.

24. Sixthly, the Prevention of Money Laundering Act of 2002 provides a foundation for determining the genuineness of customers who utilize the services of the bank. The Rules published under this Act with relevance to identity of clients i.e., Rule 9 of the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining

and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 makes it mandatory to verify records of the identity of clients. Rule 9 reads as follows:

> (1) Every banking company, financial institution and intermediary, as the case may be, shall,(a) at the time of commencement of an account-based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship, and
> (b) in all other cases, verify identity while carrying out:
> (i) transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or
> (ii) any international money transfer operations.
>
> (1 A) Every banking company, financial institution and intermediary, as the case may be, shall identify the beneficial owner and take all reasonable steps to verify his identity.
>
> (1 B) Every banking company, financial institution and intermediary, as the case may be, shall exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the customer, his business and risk profile.
>
> (1 C) No banking company, financial institution or intermediary, as the case may be, shall keep any anonymous account or account in fictitious names.

> Apart from several other sub-clauses to this, sub-clause 7 (ii) reads as follows:
> '(ii) Every banking company, financial institution and intermediary as the case may be, shall formulate and implement a Client Identification Programme to determine the true identity of its clients, incorporating requirements of sub-rules (1) to (6A) and guidelines issued under clause (i) above.'

It is pertinent to note that the respondent bank appears not to have taken these directives very seriously. Apart from relying on a checklist of routine documents on the identity of the client, establishing the genuineness of the customer who has utilized the banking system of the bank to perpetrate the fraud over the internet has not been sufficient. The realization that the customer who indulged in the fraud has ceased to function from the business premises for a long period of time prior to the incident has arrived rather late. Further, even after the occurrence of the incident, the response in identifying the customer

who has indulged in this fraud has been lukewarm. The respondent bank has not initiated any action on the customer who has brought discredit to the banking system of the bank and this gives the impression either that the bank does not take harm dealt to its customers via its own banking system seriously or again leads to the assumption of the possibility of a certain degree of complicity of the bank branch.

25. Considering all the factors listed above that combine to influence the conclusion that the Respondent Bank namely ICICI has failed to establish that due diligence was exercised to prevent the contravention of the nature of unauthorised access as laid out in Section 43 of the Information Technology Act of 2000, I find the petitioner justified in the instant case. The Respondent Bank has failed to put in place a foolproof Internet Banking system with adequate levels of authentication and validation which would have prevented the type of unauthorised access in the instant case that has led to a serious financial loss to the petitioner customer. The basic loophole in ensuring that a customer recognizes an email as from the bank was a glaring error on the respondent's part that would have prevented this incident. The degree of connivance or complicity may be debated upon but the neglect of the personnel of the Respondent Bank both immediately prior to and immediately after the loss in protecting the interests of the customer are clearly evident. Adequate checks and safeguards have not been planned together with the fact that the effort to investigate and track the perpetuator of the fraud who was a subject of its own procedures in being made a customer are seen to be poor. The Know Your Customer norms have been violated in letter and in spirit. The petitioner has been made to run around in search of justice and retribution following the incident without any support from the bank. The Respondent Bank is found guilty of the offences made out in Section 85 read with relevant clauses of Section 43 of the Information Technology Act of 2000.

26. As regards, the quantum of compensation, attention is drawn to section 47 (b) of the Information Technology Act of 2000 which is in reference to the same and states that due regard shall be had to the quantum of loss suffered as a result of the default.

a) In the instant case, of the Rs.6,46,000/- in his bank account, the petitioner customer has suffered a financial loss of Rs.4,60,000 due to this incident that was drawn over the counter as cash by Uday enterprises and Rs.35,000 adjusted by the Bank itself against the dues of Uday enterprises. A sum of Rs.1,50,171/- has been re-credited to the petitioner customer's account by the bank. Hence, the net financial loss to the petitioner customer is Rs.4,95,829/-

b) If this amount of Rs.4,95,829/- is computed at 12% simple interest per annum (minimum bank interest rates for loans) from the date of financial loss suffered

by the petitioner viz., 6th September 2007 upto the date of issue of this judgment for a period of 2 years and 7 months, then it would work out to Rs.1,60,648/-.

c) Further, the total fee (Advalorem fee and Application fee) that had been paid by the petitioner as applicable statutorily for adjudication on account of the incident that lead to the financial loss was Rs.27,850/-.

d) Also, the petitioner has had to travel several times from his workspot in Abu Dhabi to India to file and follow up on the case at different offices and also before this adjudicating officer and due to this to suffer further financial loss on account of complete lack of involvement of the respondent bank and all these travel and incidental expenses are computed on a lumpsum basis as Rs.6,00,000/-. Therefore the total amount that is expected of the respondent bank to pay the petitioner for all the losses suffered by him is Rs.12,84,327/- (Rs.4,95,829/- + Rs.1,60,648/- + Rs.27,850/- + Rs.6,00,000/-) rounded to **Rs.12,85,000/-.**

Thus, the respondent bank namely ICICI in the instant case is directed to pay a total sum of Rs.12,85,000/- (Rupees Twelve Lakhs Eight five Thousand only) to the petitioner within 60 days from the date of issue of this judgment.

The application for adjudication is ordered with the above direction.

12/4/10

(P.W.C. DAVIDAR, IAS)
Adjudicating Officer and
Secretary to Government
Information Technology Department
Government of Tamil Nadu

P.W.C. DAVIDAR I.A.S

INFORMATION TECHNOLOGY ACT 2000
Secretary to Government
Information Technology Department
and
Adjudicating Officer
GOVERNMENT OF TAMIL NADU

Secretary to Government
Information Technology Department
12 APR 2010
Chennai-9