PHISHING ATTACK AND DATA PROTECTION

B. Gopalakrishnan
President & Head Legal
Axis Bank Limited

August 2013

Phishing attack and data protection - a Case Study

For the first time in the history of India, the new Companies Bill which got passed in both the Houses of Parliament and waiting for the assent of President and Gazette Notification, the term "fraud" has been defined under Article 447 of the Companies Bill. The said definition reads as under.

> *"fraud" in relation to affairs of a company or any body corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interest of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss;*
>
> *"wrongful gain" means the gain by unlawful means of property to which the person is gaining is not legally entitled;*
>
> *"wrongful loss" means the loss by unlawful means of property to which the person losing is legally entitled.*

The above is a comprehensive definition.

The relevance of the said definition to Banks as on date is a virgin area because in India, we have two types of banks, even though they conduct the same business. There are the PSUs, which are constituted under an Act of Parliament and others also are constituted under the Companies Act as in existence from time to time. However, both set of banks are governed under the Banking Regulation Act, 1949 and the said Act stipulates that in case of conflict, the provisions of Banking Regulation Act, 1949 shall prevail. Unfortunately, the Banking Regulation Act, 1949 has not defined the term "fraud" with respect to Banks, be it public sector or private sector, and same is drawn from the dictum laid down by RBI through its circulars from time to time.

Therefore, an act of omission or commission which may fit in as fraud in the definition of fraud under the new Companies Act may or may not classify as a fraud if the same does not fit in the classification as defined by RBI from time to time, the same can apply vice versa also.

Therefore, it is high time RBI revises its classification of fraud to include the definition of fraud as per the new Companies Act. Failure to do so may simply lead to litigation warranting an interpretation by courts to settle the said dispute.

While I am aware that the definition of fraud, as classified by RBI, is with respect to the fraud committed by a Bank employee or a third person with respect to a customers' account, the definition of fraud as defined in the new Companies Act is with respect to or more leaning towards the fraud committed by the Company as a whole which will affect the shareholders. The inclusion of the said definition will act as a big boost to RBI to examine the truthfulness of the accounts prepared by the Banks to a great extent, even though the formatting is different with respect to certain issues.

Having said so, the most important type of frauds which the customers of a Bank have to face is the cyber crime, which is called in various names like phishing attack whereby money is transferred from the account of a customer without human intervention. I give here a case study.

> *A complaint was received by one of the banks from its customer alleging withdrawal from his two accountsviz. Rs.9,42,000 lacs from one SB account and Rs.1,74,500/- from another account on 30.03.2012 and 31.03.2012 and complained of phishing attack in the accounts. Upon enquiry, it was revealed by bank that out of Rs.942000/-, Rs.200000/- each had been transferred through NEFT to accounts maintained with other two banks. When the matter was taken up with these two banks, the balance available in the said accounts was Rs.94000/- with one bank and with another bank was onlyRs.25000/- as informed by the said banks. Further, some amounts were also transferred to other accounts of the Bank, where complainant was holding the account.*
>
> *On enquiry, the complainant informed that his mobile service provider had issued duplicate SIM card around 30.03.2012 and his original SIM was deactivated, based on request by somebody and due to this reason, he did not receive any SMS informing passwordsfor the said transaction as also the confirmation of the transaction carried out on the said dates.*

In the aforesaid case study, in fact, the fraudsters logged into complainant's account using login ID and passwords and other details and further using the duplicate SIM card procured in the name of the Complainant, carried out the said transactions by using the password for each transaction received on duplicate SIM card. It was informed by complainant that he had not applied for duplicate SIM card and hence, it is the mobile service provider, who without following any proper checks and procedures or without confirming whether the actual customer has approached them for duplicate SIM or without conducting basic due diligence, blocked the SIM card of the Complainant and issued Duplicate SIM card to unknown persons/third parties and handed over the same to such unknown persons/third parties and in such case, the bank cannot be held liable or responsible for alleged fraudulent

transactions made in the account of complainant by such unknown persons/third parties with the help of duplicate SIM card issued by mobile service provider. There was no fault in the bank's systems and procedures.

In the given circumstances, it is found that Regulator, Adjudicator, Court conveniently forgets to take note of this and makes the Bank responsible or liable for the alleged fraudulent transactions in the accounts of customers.

The other most important type of fraud which is happening is the ATM frauds where the innocent customers, who come to withdraw money unknowingly surrenders his or her vital personal data to the fraudster,who uses it effectively elsewhere by conning the same and cleans up the savings.

As on date, there are multiple foras which deals in this issue. Some may go to Consumer Forum, some may file a civil suit, some may file complaint with cyber cell of the police under Criminal Act, so may go to adjudicate the same under section 46 of the Information Technology Act, 2000.

The availability of the multiple Fora is not a boon but a curse as it will only create confusion and chaos in the field and neither the customers nor the Bank will benefit.

In my considered view, the issues as contained in the above two types of cases cannot be termed as a deficiency of service as defined under the Consumer Protection Act, 1986 nor do the Learned members of the Fora have the expertise to decide on the case. The jurisdiction of the Fora with respect to such cases should be expressly barred.

In this connection, it is pertinent to have a look at the rules framed by the Ministry of Communications and IT and gazetted on 11.04.2011.

Section** 43A **of Information Technology Act, 2000

"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 so affected.

Explanation — For the purposes of this section,—

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or association as it may deem fit."

In terms of the said section i.e. 43A (III), Government of India has now come out with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 ("IT SPD Rules") with regard to the definition of sensitive personal data or information.

The most interesting part of this section is that, it also protects the Bank when the Bank gives such personal data to any outside agency for an outsourcing purpose. Therefore, this section and regulation is not limited to the fact that such claim can arise only to banks or other intermediaries, it can arise to the outsourced entity also.

On the given background, we now analyze the contents of the IT SPD Rules formulated by Government of India, Ministry of Communication and Information Technology.

The said IT SPD Rules relates to dealing with information generally, personal information and "sensitive personal data or information" ("hereinafter, SPD"). The term 'reasonable security practices and procedures' means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be specified in any law. The major points of IT SPD Rules are described below for ready reference:

1. Sensitive Personal Information: SPD is defined to cover the following: (a) passwords, (b) financial information such as bank account or credit card or debit card or other payment instrument details; (c) physical, physiological and mental health condition; (d) sexual orientation; (e) medical records and history;

and (f) biometric information. It may be noted that SPD deals only with information of individuals and not information of businesses.

2. Privacy Policy: Every business is required to have a privacy policy, to be published on its website. The privacy policy appears to be required whether or not the business deals with SPD. The privacy policy must describe what information is collected, the purpose of use of the information, to whom or how the information might be disclosed and the reasonable security practices followed to safeguard the information.

3. Consent for collection: A business cannot collect SPD unless it obtains the prior consent of the provider of the information. The consent has to be provided by letter, fax or email. The business must also, prior to collecting the information, give the option to the provider of the information to not provide such information. In such case, the business can cease providing goods and services for which the information is sought.

4. Notification: The business should ensure that the provider of the information is aware that the information is being collected, the purpose of use of the information, the recipients of the information and the name and address of the agency collecting the information. Prior consent is required for disclosure of the information to any party other than the government.

5. Use and retention: The business can use personal information only for the purpose for which it was collected. Also, the business cannot retain the SPD for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law.

6. Right of access, correction and withdrawal: The business should permit the provider of the information the right to review that information and should ensure that any information found to be inaccurate or deficient be corrected. The provider of the information also has the right to withdraw its consent to the collection and use of the information.

7. Transnational transfer: A business can only transfer the SPD or information to a party overseas if the overseas party ensures the same level of protection provided for under the Indian rules. Further, the information can be transferred only if it is necessary for the performance of a lawful contract between the body corporate and the information provider or where the information provider has provided his consent to such transfer.

Security procedures: The IT Act requires reasonable security procedures to be maintained in order to escape liability (see above). The rules appear to state that

reasonable security procedures would be either (a) the IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements; or (b) a code developed by an industry association and approved and notified by the government. The security procedure has to be audited on a regular basis by an independent auditor, who has been approved by the Government of India. Such audit should be carried out at least once a year or as and when the body corporate has undertaken a significant upgradation of its computer resource.

In the given circumstances, are the Banks held liable and made to pay for the internet or phishing attacks, especially if the Banks have taken reasonable and due care as is stipulated by RBI ?Are not the Banks being unfairly targeted for no fault of the banks where in the given cases, bank itself is a victim u/s 43 and not the perpetrator of the crime.

Recently, the media reported about the Adjudicating Officer ordering to the banks to make the payment in the given below case.

> *Complainant was holding a savings account with private bank. An amount of Rs.14000/- was withdrawn from her account from ATMs of two banks in Gujarat, however, complainant alleged that at the time of these withdrawal transactions, she was in physical possession of her debit card and she had never been to Gujarat.*
>
> *In order to withdraw cash from an ATM, one should possess the ATM card of the account holder and should also be having knowledge of the PIN number, which is known only to the customer. Unless a person is having these two vital materials, he cannot withdraw the amount. In this case the transaction was successful as the alleged culprit was in possession of these two i.e. card and PIN number. The fact that someone had withdrawn money in normal course from any ATM does not fall under both these sections as the complainant was an account holder of another bank and the banks, where withdrawals had taken place, were not in possession of any data of the complainant.*
>
> *The complainant filed a complaint with Commissioner of Police and in response to complaint, the banks, where the alleged fraudulent withdrawals had taken place, were asked to provide CCTV footage of the concerned ATMs. CCTV footage was provided by one of the banks, which showed an unindentified person withdrawing the amount with his face covered, however, the quality of the same was low. The other bank did not have CCTV footage as the data was overwritten after a period of 3 months.*

The Order was passed against the two banks, where alleged fraudulent withdrawal had taken place in violation of Section 43A of IT Act and they were asked to pay compensation of Rs.20000/- to complainant.

The above order is bad in law and is not a case coming u/s 43 to be adjudicated under IT Act, 2000.

In the said case, it is a clear case of a crime which does not come u/s 43 of IT Act, 2000. However, the adjudicating officer went ahead and passed an Order treating it as a violation u/s 43 & 43A of IT Act.

To conclude, while we have progressed and advanced much into technology platform and can conquer the world by the click of a button, the days of privacy is also over. Banks and customers have to be alert at all times and there exists no foolproof one time solution to the problems of cyber crimes that are rampant.

The grave nature of the problem is evidenced when the author have had a chance to discuss the case of a cyber crime i.e. phishing attack with the IG of police heading the Cyber Cell of a State, which has advanced in this technology. The IG, with a wide grin, told me that he never trusts internet transactions and always writes a cheque.

**********_____**********