Case Study
When Customer Care Turns into a Customer's Nightmare

Dr. H. R. Venkatesha
Director, Acharya Bangalore B-School, Bengaluru.
Prof. M. Viswanathan
Professor, Department of Management Studies (PG), Acharya Bangalore B School (ABBS), Bengaluru, Karnataka.

ABSTRACT

Many of us opt for Credit Cards provided by various banks for the convenience it extends in making purchases on credit with no interest for a limited period and various other offers attached to it. The customer care rendered in giving this service is more or less similar with all the banks. What we take for granted is the various security barriers that the banks employ to protect the customer while making financial transactions. What we are unaware is the quality of these security barriers which we associate with the brand name, reputation and credibility of the bank we choose. No customer knows to what extent the data he gives the bank when filling the application form and other information that the banks emphasize that the customers should keep confidential leaks into the public domain till he / she experiences a breach in the security barriers that is meant to protect the customer. That is when the customer is exposed to the fraudulent transactions in his / her card due to negligence arising from irresponsible conduct by the customer or by the impact of external factors in digital transactions beyond the control of individuals. These are described as cyber crime in digital marketing. This case study is based on the real time experience of Victor (Pseudonym) as a victim of cyber crime in credit card based transactions. The purpose of this case study is to share Victor's experience as a victim of cyber crime and reveal the inadequacies in the electronic financial transactions in India with particular reference to credit / debit card based transactions in digital marketing and expose the attitude of the service provider, namely the concerned bank (Bank X) (identity not revealed), in withdrawing their customer support at such a crucial juncture, thus turning customer care into a customer's nightmare. The steps to be taken by the victim to mitigate the impact of cyber crime has been given in detail as prescribed by the Cyber Crimes Cell. The steps to be taken in seeking relief as recommended by the bank as service provider has been stated under 'Escalation Matrix' in the study. In addition, precautions to be adopted in card based transactions has also been discussed.

Key Words: Security Barriers, Cyber Crime, Electronic Financial Transactions, Customer Care, Escalation Matrix.

1. Introduction

The global quantitative impact of cybercrime is estimated in 2018 to be over US$1.5 trillion **(Cybercrime Statistics)**[1]. The cyber crime investigating agencies state that at least one cyber crime is reported every 10 minutes in India **(One Cyber Crime in India Every 10 minutes)**[2]. Cyber crime cases in India, registered under the IT Act, increased at the rate of 300 percent between 2011 and 2014 **(Cybercrime in India - Wikipedia)**[3]. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 44679, 49455, 50362 and 53081 cyber security incidents were reported during the years 2014, 2015, 2016 and 2017 respectively **(CERT-In : Report 2018)**[4]. Also, the rate of arrests in cybercrime is said to be abysmally low. For instance, the National Crime Records Bureau (NCRB) said in its 2016 report (for 2015), that of the cases of cyber crime which were registered in India,

only 8,121 cases lead to arrests. This is because law enforcement agencies were observed to be not well-equipped and properly oriented towards cyber crime **(NCRB Report 2015)**[5]. Hence, there is a compelling need for quality training **(Cybercrime Investigation - A Long Way to Go)**[6]. Bengaluru registered the most number of cybercrime cases in 2018 amounting to filing of a massive 55,035 FIRs being registered at the cybercrime police station in the city **(Bengaluru Cybercrime Capital)**[7]. This has been attributed to an unprecedented increase in online criminal deceptions that have become a daily occurrence. Each day, thousands of innocent individuals fall prey to online banking and credit/debit card frauds. Losing one's hard earned money to online criminals can be a painful, hard to accept and psychologically draining traumatic experience to the victim. This case study is based on real time experience of Victor (Pseudonym) as narrated to the authors when he became a victim of fraudulent transactions on his credit card. The sensitive nature of the case requires the authors not to reveal the identities of the victim (Victor), the concerned bank, (Bank X) and Personnel at the Cybercrime Investigating Cell, without compromising on the facts of the case in the narration.

2. THE CASE JOURNEY - "HOW IT ALL STARTED"

Victor planned a foreign trip in July 2018. The booking was done with an online ticketing agency Pleasant Trip (Name Changed). The air ticket payment was made online using Victor's credit card of Bank X. The E-Ticket established the fact that Victor would be out of the country from Friday 20th July 2018 to Friday 27th July 2018.

The July 2018 Credit Card Statement of Bank X came to Victor's e-mail on 18th Aug 2018.

On examining the Credit Card Statement, three (3) debits were identified as transactions that Victor did not authorize, and therefore, fell into the category of unauthorized fraudulent transactions. They were made on 23rd July 2018 in India. The vendors were Indian companies and the transactions were consecutive as described below. The transactions are given in the same order as it appeared in Victor's credit card statement of Bank X.

S. No.	Particulars	Amount (Rs.)
1	Flipkart Internet Pvt Ltd., Books and Stationery	Rs. 65,088
2	Paytm, Noida, India Mobile Phones and Bill Payment	Rs. 20,000
3	Flipkart Internet Pvt Ltd., Books and Stationery	Rs. 61,990
	Total	**Rs.1,47,078**

Victor surmised from the above statements that there had been a breach of security on his Credit Card which called for immediate actions to be taken to pre-empt further abuse. The steps prescribed by the authors are based on the guidelines adopted by Victor in reporting the cyber crime

(How to Register Cyber Crime Complaint with Cyber Cell of Police)[8]

2.1 Immediate Steps Taken

- Called Help Line of Bank X and blocked the Credit Card from further use.
- Filed FIR and obtained attested FIR copy from Cyber Crimes Branch.
- Downloaded Dispute Form of Bank X (Dispute Form)* and filed details of the transactions in dispute.
- Attached FIR copy to the Dispute Form of Bank X and uploaded it in Bank's Website.
- Called Help Line of Bank X and informed the actions taken.
- Bank X acknowledged receipt of documents by return email with a Case Reference No.
- A detailed email with facts was prepared and uploaded to Customer Care of Bank X.
- Copies of the email to Customer Care was sent to CEO and CFO of Bank X

** A Dispute Form is a questionnaire of Bank X that enquires into the details of the unauthorized fraudulent transactions. Victor tick (✓)marked the following option (given verbatim) that best represented his true position in the disputed transactions.*

(✓) I have not participated or authorized the above transaction(s). The card was in my possession at all times. www.disputeform-BankX.com (True website identity not revealed).

2.2 Facts Presented to Customer Care (Credit Cards) of Bank X

- The Credit Card was in customer's (Victor's) possession during the disputed transactions.
- The customer did not authorize any of the disputed transactions on 23rd July 2018.
- Indian SIM Cards become non-operational outside India.
- Consequently, the OTP and transaction alerts could not have reached the customer's SIM.
- There has been a security breach in the barriers to protect the customer against the fraud.
- There was no email alert of the transactions on customer's email ID registered with Bank.X.
- SMS message records till flight departure time on 19 July 2018 - proof that SIM was with customer.
- SIM Card being re-activated in India on 28th July 2018 on arrival - additional proof.
- Outgoing mobile calls and SMS records showed 'NIL' during 20 - 27 July 2018. (Telecom Regulatory Authority of India (TRAI))**
- Immigration Stampings on customer's passport confirmed that he was abroad at the time.
- Purchases abroad using the Credit Card recorded in the credit card statement of August 2018 was proof that credit card was in customer's possession.

With above facts as proof, Victor sent an email to Customer Care expressing his displeasure on the security breach and the resulting mental trauma arising from the fraudulent transactions. Under the circumstances, Victor requested Customer Care of Bank X to reverse the transactions.

***According to TRAI, Mobile Service Providers in India can give their customers a record of only outgoing calls and SMS messages against a prescribed fee. Incoming calls and SMS messages are kept confidential and can be shared only with designated competent authorities for security reasons. https://main.trai.gov.in*

Response from Bank X on the Disputed Transactions

The response from Bank X is presented below verbatim

Mon, Sep 17, 2018 at 2.00 pm

Dear Sir,

Thank you for your email. I understand that you seek clarification regarding fraud transaction done on your card. As per the confirmation received from the team, the card has to be blocked within seven days of fraudulent transaction taking place. As we are checking card is blocked after 7 days. Thus we are unable to take up the case with further investigation.

Best regards
Customer Care - Bank X

3. RBI GUIDELINES FOR CARD BASED FRAUDULENT TRANSACTIONS - EXTRACT OF SALIENT FEATURES

With the increased thrust on financial inclusion and customer protection and considering the recent surge in customer grievances relating to unauthorized transactions resulting in debits to their accounts/ cards, the criteria for determining the customer liability in these circumstances have been reviewed. The revised directions in this regard are set out below.

3.1 Strengthening of Systems and Procedures

- The systems and procedures in banks must be designed to make customers feel safe about carrying out electronic banking transactions. To achieve this, banks must put in place appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers that includes ;
- Robust And Dynamic Fraud Detection and Prevention Mechanism;
- Mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorized transactions and measure the liabilities arising out of such events;
- Appropriate Measures to mitigate the risks and protect themselves against the liabilities arising therefrom; and
- A system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

In order to achieve this;

Banks must ask their customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions. The customers must be advised to notify their bank of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction.

In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to transaction value or the amount mentioned, whichever is lower.

- Credit cards with limit up to Rs.5 lakh Maximum liability Rs. 10,000/-
- Credit cards with limit above Rs.5 lakh Maximum liability Rs. 25,000/-

Further, if the delay in reporting is beyond seven working days, the customer liability shall be determined as per the bank's Board approved policy. **(RBI NOTIFICATIONS - RBI/2017-18/ 15DBR.No.Leg.BC78/09.07.005/2017-18; 6/7/ 2017- Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions reporting of unauthorized transactions by customers to banks)**[9]

3.2 Policy on Billing Disputes - Excerpts from Customer Handbook of Bank X (Based on RBI Guidelines)

Billing Disputes - All contents of the Statement(s) will be deemed to be correct and acceptable by the Cardholder(s) unless within 21 days of the Issue of Statement, the Cardholder informs the Bank of any discrepancies. If the aforesaid discrepancies are found to be legitimate by the Bank, it may reverse the charge on a temporary basis until the completion of subsequent investigations by the Bank to its full and final satisfaction. **(Customer Handbook of Bank X - Most Important Terms and Conditions)**[10]

4. Policy of Bank X on Customer Protection in Electronic Banking Transactions

The policy outlines the obligations on behalf of bank and customer to ensure the onus of liability arising out of fraudulent transaction.

4.1 Customer Protection: Limiting Liability of Customers in Unauthorized Electronic Banking Transactions - Customer centricity is one of the core values of the bank. Bank X truly believes that Customer Experience is the key to keeping customers happy and thereby ensuring a long lasting relationship with the Bank.

4.2 Objectives of Bank X in Electronic Banking Transaction

- To ensure that the systems and procedures in bank X are designed to make customers feel safe and secure while carrying out electronic banking transactions by themselves;
- To install robust and dynamic fraud detection and prevention mechanism to prevent abuse
- To take appropriate measures to mitigate risks and protect themselves against liabilities arising thereon;
- To devise a system to continuously educate customers in protecting themselves from frauds arising from electronic banking and payments.

4.3 Bank Must Ensure Following:

- Appropriate systems and procedures to ensure safety and security of electronic banking transactions;
- Dealing quickly and empathetically with customer grievances;
- Mandatorily ask customers to register for SMS and wherever available register for E-mail alerts for electronic banking transactions;

Mandatorily Send SMS and wherever available, Send E-mail alerts for electronic banking transactions and advice customers to notify unauthorized electronic banking transactions to Banks instantly upon occurrence.

4.4 Summary of Customer Liability: If the delay in reporting is beyond 7 working days, the customer liability shall be determined as per the bank's Board approved policy. Beyond 7 working days Full Liability of the fraudulent transactions will lie with the customers. However, customer will be compensated up to a limit of Rs.5000/- or the transaction value, whichever is lower, only once in the lifetime of the account as per Bank's Board approved compensation policy.

4.5 Third Party breaches are where the responsibility for the unauthorized electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay of 4 to 7 working days on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned, whichever is lower.

- Credit cards with limit up to Rs.5 lakh Maximum liability Rs. 10,000/-
- Credit cards with limit above Rs.5 lakh Maximum liability Rs. 25,000/-

4.5.1 Third Party Breaches would cover following unauthorized transactions that have taken place without customer's knowledge

SIM Duplication -

- Cloning of original SIM to create duplicate SIM
- Application related frauds- Stolen customer identity which is used to avail bank's products and services;
- Account Takeover- Theft of account information to obtain banks products and services including extracting funds from the customers bank account;
- Skimming/Cloning - Collect data from the magnetic strip of the card and copying the information onto another plastic. **(Policy of Bank X on Customer Protection in Electronic Banking Transactions)**[11]

5. VICTOR'S REJOINDER TO BANK X

The inference drawn from the response of Bank X indicated that the bank was avoiding the responsibility of investigating the unauthorized fraudulent transactions. They wanted the customer to cough up the money involved in the unauthorized transactions done on his credit card. This was unacceptable. A befitting retort by email was sent by Victor to Bank X which is given below verbatim.

To: Customer Care, Bank X, Sep 18, 2018

Sir, Thank you for your email dated Sep 17, 2018.

I wish to bring to your kind attention that my SIM was non operational for the period 20 - 27 July, 2018 as I was out of the country at the time. I am once again attaching the scanned copies of my passport stampings and call records of my SIM as proof.

I am once again reiterating that both the SIM and the Credit Card were in my possession. The call records of my SIM card are adequate proof that the SIM card was in my possession. Please see the call and SMS records on 19th July 2018 till my flight departure time, no call and SMS records for the period 20 - 27 July 2018, and call and SMS records from 28th July 2018 after reactivation of the SIM in India after arrival. These are clear indications that the SIM Card was in my possession and that there were no third party breaches on my SIM card such as cloning.

The purchase records on my credit card statement indicate overseas purchases on 20th July 2018 and 27th July 2018, which are adequate proof of credit card being in my possession.

Hence, if there was an OTP alert, there was no SIM to receive it. So who authorized these transactions? How did your transaction team process these 3 transactions without any OTP approval? How was the payment made when the credit card was in my possession? These are queries you should be asking your transaction team to reply. With no transaction alerts, the 7 day grace period you have specified in your email is irrelevant, unreasonable and hence, untenable, as these transactions have violated the security barriers that your bank has to provide the customer. I once again reiterate that these transaction have taken place without my approval. Therefore, without any further harassment, I request you to kindly reverse the transactions.

Thank you.
Regards.
Victor

6. THE ESCALATION MATRIX

Bank X responded to Victor by prescribing the Escalation Matrix as a solution to address the issue. The steps in the process are given below.

Step 1 - In case, the query remains unresolved for more than 10 days or no update provided by Customer Service team or the Branch, you may write to nodal.officer@bankX.com along with complaint no.

Step 2 - The complaint remains further unresolved for 10 days or no update is provided by the Nodal Officer, kindly write to circlenodalofficer.bangalore@bankX.com

Step 3 - The complaint remains further unresolved for 10 days or no update is provided by the Circle Nodal Officer, you may escalate to Principal Nodal Officer pno@bankX.com

Step 4 - Even after following the above process, the complaint remains further unresolved for 30 days, then you may write to RBI - Banking Ombudsman in the city bobincity@rbi.org.in

7. THE BEGINNING OF CUSTOMER'S NIGHTMARE

During first week of September 2018, Victor settled the outstanding dues on his credit card minus the disputed transactions. Since the credit card was blocked, no transactions were made and the only outstanding that remained were the transactions in dispute. Towards the third week of September 2018, the new credit card statement for August 2018 came to Victor's email. An interest of about Rs. 20,000/- was added to the disputed transactions and the outstanding balance stood at around Rs.1.67 lakhs. Call to Customer Care indicated that investigation into Victor's case was going on and till then the outstanding balance would remain and interest would be added to this on a monthly basis.

From October 2018, Victor started getting calls from the Credit Card Division of Bank X on a daily basis asking him to settle the outstanding amount. When Victor responded that Custom Care indicated investigations were going on, the Credit Cards Division said that they were not aware of any investigations being carried out and that it would be in the best interest of the customer to settle the outstanding dues immediately to avoid legal action from the bank. Meanwhile the Credit Card Statement for September 2018 was released to Victor's email during the third week of October 2018. The outstanding balance stood at Rs. 1.87 lakhs with addition of Rs. 20,000 /- as interest. Meanwhile, Victor to his dismay found that the first two processes listed in the Escalation Matrix yielded no tangible results for over 30 days.

With no written communication from Bank X to indicate that the bank has posted the unpaid transactions as fraudulent in nature and investigations were going on, Victor was left in a state of suspense not knowing what to do next. Calls to Customer Care at that point indicated that since the card was blocked after 7 days of the disputed transactions, the customer would be required to settle the amount as per Bank's policy. They also stated that the outstanding balance could be converted into an EMI. Victor then realized that the investigation that Bank X promised was simply a hoax to buy time. Meanwhile calls from the Credit Cards Division was adding further pressure. There was no empathy from Customer Care of the bank. Both the CEO and CFO of Bank X did not respond to Victor's email. Tension was also building up in Victor's home as to how this huge outstanding amount was going to be settled. No relief was in sight. The situation was slowly turning into a customer's nightmare.

8. INTERVENTION OF RBI

In such situations, it is important for the affected individuals not to despair. Although Victor was emotionally drained, he rationalized that the situation required a different approach. He reviewed the Escalation Matrix suggested by Bank X. Since the response of the bank was unsatisfactory he decided to meet the Banking Ombudsman of RBI in the city in the third week of October 2018 and intimate him / her about the case with all the supporting documents. At the meeting, the RBI ombudsman promised to get back within a fortnight.

9. INTERVENTION OF CYBER CRIMES INVESTIGATIONS CELL

Victor felt that his case required intervention from a higher authority in law enforcement in order to vindicate his non-involvement in the fraudulent transactions. He reviewed all the contacts in his network. One of the contacts in his network knew one of the high ranking officials in the Cyber Crime Investigations Cell. A meeting was arranged with this high ranking official during first week of Nov 2018. Victor apprised him of his plight. The officer verified the authenticity of all the documents submitted by Victor. He was satisfied that the case was genuine. He appointed a police officer to investigate the progress in the case. The Police Officer verified the case with the FIR No. and confirmed that the vendors and Bank X had not responded to the enquiry of the Cyber Crimes Cell. Hence, the officer redrafted the email enquiry to the vendors and took a hard copy of the official enquiry to Bank X. He requested Victor to accompany him to the Regional Office of Bank X and submitted the official enquiry to the Principal Nodal Officer of Bank X and demanded a reply within ten working days.

10. THE TURNING POINT

Victor's mind was at peace at that point in time because Bank X was now officially compelled to conduct an enquiry and report the outcome to both RBI and Cyber Crimes Cell. This was evident because for the first time, Victor received a call from the Head office of Bank X, verifying the facts given by him. The call was recorded by Victor for posterity.

10.1 The First Relief came by way of an email from the Banking Ombudsman, RBI.

From: Banking Ombudsman, RBI

To: Mr. Victor

Friday Nov 16, 2018

Subject: Closure of Case - Mr. Victor, Fraudulent Transactions on Credit Card

Dear Sir: Please refer to the captioned complaint.

On perusal of the complaint Bank X has agreed to reverse the disputed amount in the complaint along with applicable charges and the same has been communicated to the complainant. In view of the above, the complaint is closed under Clause 11 (3) (a) of BOS 2006 which reads as under : "the Banking Ombudsman may deem the complaint as resolved in any of the following circumstances - where the grievance raised by the complainant has been resolved by the bank or the concerned subsidiary of the bank with the intervention of the banking ombudsman".

You are further informed that the clause under which the complaint has been lodged is closed

Yours faithfully
Banking Ombudsman

10.2 The Second Relief came by way of an email from Bank X

From: pno@bankX.com

To: Mr. Victor

Dear Sir

This is with regards to your complaint lodged at the office of the Banking Ombudsman regarding online transaction dispute of Rs. 147078 /- dated 23.07.2018 in your credit card

We wish to inform you that all the 3 disputed transactions have been done using OTP which were sent to your registered mobile number and email id. However, as a service gesture, we will be reversing the disputed transactions along with reversal of applicable charges to your credit card within 7 working days.

Assuring of our best services.

Regards,
Principal Nodal Officer
Regulatory Escalations & BO Complaints
Bank X Ltd

11. GLEANINGS FROM CYBER CRIMES INVESTIGATION IN THIS CASE

Victor visited the Cyber Crimes Investigation Cell to thank the police officer who had worked on the case. He requested further investigation into the case to nab the real culprits. The officer declined stating that since the case was officially closed there was no scope for further investigations to be taken up. However, he gave some insights into how the crime could have been

committed. Some IT professionals whom the authors contacted confirmed the findings.

- Victor's purchase of flight ticket on-line could have been the primary source of information.
- Such transactions are monitored by cyber criminals on a day to day basis by illegal means and insider information is obtained on a specific or random basis.
- These transactions become the basis for perpetrators of Cyber Crime to choose their victims after studying the demographic profile of the customer.
- Technology is applied to circumvent the barriers of OTPs, SMS and email alerts.
- Cyber Criminals are aware of the inadequacies in Cyber Crime Investigation Cell.
- Cyber Criminals are familiar with the legal loopholes.
- Criminals anticipate how victims would react and get periodic feedbacks on their moves.
- They know the work overload of investigators at Cyber Crime Investigations Cell and the infrastructure inadequacies in the system resulting in delay in the investigations.
- The strike rate of cyber crime is therefore, very high. The criminals work on a daily basis 24/7.
- The source of Cyber Crime is untraceable. If traced, it leads to many Indian and International locations.
- The criminal is a phantom - a ghost
- Communication is one way - Striker to Victim and not vice versa.
- Cyber criminals are computer savvy. They update their skills by employing the latest hacking techniques and adopt innovative ways to circumvent the system.
- Hence, professional hacking has developed into a lucrative career.
- The law enforcement agencies are unable to keep abreast with the pace of developments in cyber crime in India.

12. ANALYTICAL INSIGHTS ON CREDIT AND DEBIT CARD SECURITY IN INDIA

RBI intervention is a very important element in controlling card based cyber crimes in India. In this regard, the time period to report an unauthorized transaction becomes a crucial factor. RBI stipulates that the customer should report the unauthorized transaction within 7 days of its happening. In the opinion of the authors, this policy guideline needs to be reviewed. When perpetrators of cyber crime have devised technological tools to circumvent the security barriers of OTP, SMS, and email alerts, the customer will become aware of the fraudulent transaction(s) only upon receiving the updated statements which would normally take place once a month. Hence, a 60 day time period to report a fraudulent transaction would give the customers sufficient time to become aware of the transactions of dispute and report the incident.

Credit and debit cards play a major part in revenue generation activities of a bank. In card based transactions, banks in India are using the security systems of the agencies established by multinationals such as Visa, Master Card, Diners Club etc., When fraudulent transactions are taking place on a daily basis on credit and debit cards, the concerned banks should be holding the agencies providing the security barriers responsible for the lapses and not pass the buck to the customers. When marketing credit and debit cards to customers, the security features in the cards are the major selling points of the bank, assuring the customers that their transactions are safe and secure. Therefore, if the customer disputes a credit / debit card transaction as being unauthorized, the burden of proof should lie with the bank to prove that the customer acted fraudulently and was complicit in the fraud or shared sensitive information about the card. Until this is done, the disputed amount should be put in a suspense account. But when a customer becomes a victim of a fraudulent transaction because of failure in the security system of the agencies, the serving

banks should desist from squarely blaming the customer and making him / her responsible for the settlement. This is not a fair practice. Such a move breaks the trust the customer has on the bank and gives scope for cyber crimes to thrive.

To be fair to the banks providing card based services to customers, the authors attribute the hostile behavior of the banks towards customers reporting disputed transactions, to the rise in the number of cyber crimes being committed on digital transactions of the bank on a daily basis. It is quite possible that the concerned banks do not have the means to cope up with this menace and therefore, all of them simply follow the RBI regulatory guidelines and pass on the burden of proof to the customers. Therefore, caution the authors, the cyber victims must equip themselves with all the facts in the case to prove their innocence. The authors also advocate an unwavering, resolute stand when presenting their case to the concerned authorities. The body language of the customer should manifest confidence. Any inconsistencies and hesitations they express in their statements in written and oral communications with the authorities namely, the bank, the police, or the RBI could work against them. This is because, on the flip side, there are also unethical customers, trying to dupe the banks for monetary gains through orchestrated fraudulent digital transactions.

The authors ponder over the fact that Victor was able to prove his innocence because he was able to establish the fact that he was out of the country at the time the transactions occurred by presenting the stampings in his passport as proof. Indian SIM Cards do not work outside India. Therefore, there was no way he could have received the OTP and SMS alerts of the transactions on his SIM Card. Yet Bank X claimed that the transactions went through the process of OTP, SMS and post transaction email alerts. Then to which mobile number was the OTP and SMS alerts diverted? To which email ID were the post email transactions sent? On what basis the vendors sent the goods and to which address? All these questions will remain unanswered forever because of the investigative weakness in the system.

13. LESSONS LEARNT AND PRECAUTIONS TO BE TAKEN

Digital transactions will become a way of life in India and will be on the increase in the years to come. Consequently, cyber crimes will also increase. The cyber criminals will continue to remain incognito and will strike at their preys in novel ways. The present system in India is inadequate to cope up with the evolving nature of cyber crimes. This is the bitter lesson the authors learnt from studying Victor's case. It is essential for individuals involved in electronic transactions, especially card based transactions, to be aware of the precautions they should adopt when they are using credit or debit cards to draw money or make payments. The owners of credit or debit cards must understand that the personal information that they have given to obtain the card is already available in the public domain to all call centers promoting various products and services. Cyber crime perpetrators, use this data to identify their victims on a random or specific basis and study the demographic profile and other factors to assess the suitability of the target to strike. When the victim is identified, they call him / her on the given mobile number and pose as customer care of the service provider bank, spin a story and get confidential information on the card such as the PIN or CVV number at the back of the card. The banks frequently advise their customers not to divulge this vital information to strangers as this would lead to abuse of their card for fraudulent withdrawal of money. This apart, the confidential information required to effect the fraudulent transactions can be obtained with the complicity of the employees of the banks when they are part of the cyber crime network. There are also other means by which confidential information on the card can be obtained through cloning devices installed in ATMs and swiping machines. Some of the general precautionary measures which can be adopted by card owners is listed below.

- Lower the upper limit of the credit card to mitigate the impact of fraudulent transactions.
- Link Card to e-banking in order to get daily updates.

- Swipe cards only in reputed outlets to avoid cloning.
- Draw money only in ATMs adjacent to service provider bank to avoid cloning.
- Press the 'cancel' button before and after cash withdrawal in an ATM.
- Cover the key board with the free hand when entering PIN for cash withdrawal in an ATM.
- Mask the 3 digit CVV number at the back of the card to prevent exposure during swiping.
- Change PIN every two months.
- Report to Customer Care when SMS and email alerts are not received after a transaction.
- Increase the periodicity of receiving e-statements from monthly to weekly.
- Opt for add on cards so that at least two persons can monitor transactions.
- Read service provider's Hand Book and Website on dealing with fraudulent transactions.

14. CONCERN OVER RECENT SECURITY BREACH ON AADHAR CARD

The security lapse involving India's national identity system the Aadhar Card indicates a disturbing trend. Aadhaar number, a confidential 12-digit number assigned to each Indian citizen as part of the country's national identity forms the biometric database of more than 90 percent of the population. The leakage of data was not a direct breach on the security of the central database run by Aadhaar's regulatory agency, namely the Unique Identification Authority of India (UIDAI), but exposes a major lapse in responsibility from the authority charged with protecting the data. Consequently, this has led to the illicit trade of citizens' data in the underground market **(Aadhar Data Leak)12**. This portends a further escalation in the intensity cyber crimes in India that would betray the trust the citizens have in the digitalization process.

15. CONCLUSION

Cyber security is a major concern for the Government of India. Lapses in cyber security cannot be wished away and swept under the carpet especially when every transaction in the country is going to be digitalized in the future. People believe in digital transactions because of the transparency it provides. However, when the very premise on which this trust is built is undermined because of the activities of cyber criminals, the citizens will begin to lose faith in the system that has been conceived to protect them. This is a dangerous trend. Therefore, the cyber security system in all electronic transactions requires major overhauling, especially in terms of policies and technology guiding and supporting the digital systems in order to plug the gaps and loop holes plaguing the digital transformation.

16. RECOMMENDATIONS

The experiential learning of the authors in coping with credit card based cyber crimes has been the basis for the recommendations stated below for dealing with hapless victims.

- RBI Guidelines Policy on the time period for reporting third party breaches by customers must be extended to 60 days instead of the present 7 days. This would be a more user friendly and customer-centric policy.
- RBI should ask the service provider banks to upgrade the technology of the agencies providing them cyber security in order to reduce the security breaches in card based transactions.
- The burden of proving the customer guilty should lie with the service provider bank. Until then the disputed amount should lie in a suspense account with no interest chargeable to either party. The service provider bank should be given no right to send communication to the customer to pay at this juncture.
- In the Escalation Matrix recommended by the service provider bank, RBI should be the first agency that victims should contact and not the last in the list.
- The banks must be given the authority to question

the vendors and elicit a response in respect of disputed transactions.

- Policy Change in TRAI in giving call records to customers: The customers must be given the right to have incoming and outgoing call records from their service provider in order to verify the receipt of security alerts in fraudulent transactions.
- The infrastructure at the cyber crime cell must be upgraded to handle the huge volume of cases received on a daily basis.
- Cyber crime investigators must be given training in the latest technologies to tackle the sophisticated methods employed by cyber criminals.
- Cyber crime cells require recruitment of more number of personnel to cope with the increasing volume of fraudulent cases.
- Cyber crime cells must seek the support of IT industry for R&D in order to keep abreast with the novel methods employed in hacking technology.

A Ray of Hope to Reinforce Cyber Security - It is heartening to note that the philanthropic arm of Infosys Foundation signed an MOU with the Karnataka Police to set up a Centre for Cybercrime Investigation Training and Research (CCITR) in Bangalore at a cost of Rs. 22 Crore that would build and maintain the facility for five years. **(Infosys Foundation To Set Up Cyber Crime Lab for Karnataka Police)**$_{13}$. Speaking to media after inaugurating the CCITR on Mar 01, 2019, the Infosys Foundation Chairperson Sudha Murthy said that the cybercrime police would be trained in tackling cyber crime cases with further training opportunities by sending them abroad to countries like the USA. **(Cyber Crime Investigators from Karnataka Can Now Hone their Skills)**$_{14}$. The authors feel that this would indeed be a new beginning to fight the menace of cyber crimes in India.

REFERENCES:

1. https://securityintelligence.com/news/cybercrime-profits-soar-to-1-5-trillion/
2. https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10- minutes/articleshow/59707605.cms
3. https://en.m.wikipedia.org>wiki
4. https://www.thehindubusinessline.com/info-tech/over-53000-cyber-security-incidents-observed-in-2018/article22705876.ece#
5. https://www.livemint.com/Politics/ayV9OMPCiNs60cRD0Jv75I/11592-cases-of-cyber-crime-registered-in-India-in-2015-NCR.html
6. https://www.rediff.com/netguide/2003/feb/18crime.htm
7. https://www.google.co.in/search?ei=SRhqXbqGOIao9QPx8rPADg & q = bangalore+cyber+crime+capital+of+india&oq = bangalore+cyber+crime+capital+of+india & gs_l=psyab.1.i39.183585.191409..194325...0.2..0.241.2845.0j15j2.....0....1..gwswiz.....0i71j0i67jj0i22i30.5x6D7qGcCaE
8. https://blog.ipleaders.in/how-to-register-cyber-crime-complaint-with-cyber-cell-of-police-online-complaint-procedure/
9. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11040&Mode=0
10. https://www.bankX.com/download/Most-Important-Terms-and-Conditiont on the d transactions.pdf
11. https://www. bankX.com/docs/default source/noticeboard/customerserviceinformation/customer-protection-policy.pdf
12. https://techcrunch.com/2019/01/31/aadhaar-data-leak/
13. https://www.thehindubusinessline.com/info-tech/infosys-arm-to-build-centre-for-cyber-crime-investigation-for-karnataka-police/article25113772.ece
14. https://timesofindia.indiatimes.com/city/bengaluru/cybercrime-investigators-can-now-hone-their-skills/articleshow/68209276.cms

.