KANININAR SERIES-PHISHING –WEBINAR- Dated 05.07.2020.

Participants Questions - Answered by

Mr. M.Sundara Kadeswaran, Advocate,Vice President, Cyber Society of India &

B.Kandasamy, Director, PPP InfoTech Ltd, www.pppindia.com

Q-1. Who is liable for enabling fraudsters? Mr.Devaraja

Answer:- Mr. M.Sundara Kadeswaran

The Question is vague. Liability can be fixed depending on facts and circumstances of each and every case.

I. Negligence of Customer

In circumstances where the bogus transaction has occurred because of the customer's carelessness i.e. the payment details or passwords were shared by the customer with someone else, then until this transaction is reported to the bank, the entire loss will be borne by the customer. However, once the transaction in question is reported to the bank, loss from any fraudulent transaction thereafter will be borne by the bank.

II. Negligence of Banking System

The customer will have absolutely no liability in circumstances where the bogus/ unauthorised transaction occurs because of the carelessness of the bank. In this case the customer doesn't even have the obligation to report the fake transaction to the bank. However, it is advisable to keep a close check on all your e-banking accounts and report any suspicious behaviour immediately to your bank.

III. Third Party Breach

When an outsider or third party commits a fraud it alludes to those situations where the inadequacy lies neither with the bank nor with the customer.

Q- *2.* Does Sec 79 of Information Technology Act, 2008(Amended) give safe harbour for intermediaries?

Dr. K.V. Gangatharan

Answer:- Mr. M.Sundara Kadeswaran

It cannot be said so as it starts with a Non Obstante Clause. If the Intermediary complies with all the statutory compliances/requirements under Section 79 (2) and related Rules framed, they can wriggle out of liability. But the onus still rests with the Intermediary.

Q -3. As a victim, who is the right person to complaint our issues in first priority or where to complaint? Also explain the timeframe of valid complaint after the incident.

Ms. *Aruvi Technologies*

Answer:- Mr. M.Sundara Kadeswaran

It is always advisable to report to the Bank first as they are expected to act first even as per the RBI Guidelines and they are expected to report to Investigating Agencies as per the Guidelines as per "Frauds – Classification and Reporting".

So far as time limit is concerned, in cases of Third Party Breach, the extent of liability of the customer depends on when he reports the issue from the day of receiving communication of such transaction from the bank.

1) If the customer reports the unauthorized exchange within 3 days from the receipt of communication

from the bank, the liability of the customer will be Zero.

2) If the customer reports the unauthorized transaction in 4 to 7 days from the receipt of communication from the bank, the customer's per transaction limit will be capped, different accounts will have different capped limit, details of which can be taken from the bank officials.

3) If the customer reports the unauthorized transaction in 7 days from the receipt of communication from the bank, the risk/ liability will be decided depending on the policies of the bank.

The number of days should be considered as per the working calendar of the home branch barring the date of receiving communication. Furthermore, the date of receiving communication implies the date when you get SMS, email or the bank explanation that gives you the knowledge about the unauthorized transaction. The earliest communication received has to be considered, on the off chance that you get communicated by the bank in various ways.The link for the relevant RBI Guideline is provided below:

https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11446

Q- 4. Do the Banks accept liability? Mr.*Devaraj*

Answer:- Mr. M.Sundara Kadeswaran

Banks clearly wouldn't want to bear the entire loss themselves and would want that the customer should share the loss be it due to the fact that the unauthorized transaction took place due to the negligence of the customer or it was the result of a third party breach, however in order to do so, the burden of proving the carelessness of the customer, is on the bank. However consult an Advocate since each case is depends up on the facts of the case.

Q- 5. I have noticed IN Play store game apps. Once a payment is done towards a game, the next ones, do not require OTP at all. It automatically gets debited once you click "pay". So in what circumstances OTP is not asked? Ms.Sheena

Answer: - Mr. B.Kandasamy

There are a few instances where OTP is not required.

1. When you are paying to a company outside India.

2. When you have entered CVV/3D secure number and saved it on the merchant site.

3. Some merchants like Flipkart have a system called Visa Safe Click which makes it possible to pay upto Rs.2000 without requiring OTP.In Google Play store you have the option to cancel/refund the purchase within 48 hours."

Q- 6. How to avoid Spam Mails? Mr. S CHOCKALINGAM

Answer:- Mr. B.Kandasamy

If you are using Gmail or Yahoo there is already an anti-spam system is in place which marks these emails into Spam folder. If you are using your own domain name then you can ask your email service/hosting provider to enable Anti-Spam settings. Most likely that option is there already which you can enable it."

Q -7. What are the different types of fraud in Phishing?

Dr.K.V. Gangatharan

Answer:- Mr. B.Kandasamy

"As mentioned in my presentation, objective of fraudster is to get your bank details or password and transfer the money. Phishing can happen in many ways using any form of digital communication."

Q -8. I have a bitter experience. I subscribed to Amazon Prime last year online through credit card by keying in the OTP received. Surprisingly when the one year period was about to lapse I got a message that my subscription will be renewed on a particular day. In case I don't want I was asked to text NO. I did so, but surprisingly it was renewed on the due date and amount was debited to my credit card, without any OTP this time. Then what is the purpose of OTP? How safe it is to make payments through online in view of such instances. Can you please throw some light as to how to protect from such automatic debit of amount? Mr.S.Balasubramanian,Advocate

Answer:- Mr. B.Kandasamy

"Only way to avoid is to Cancel the renewal or subscription prior to renewal date which can be done from your Amazon Dashboard or Payment settings. There are a few instances where OTP is not required.

1. When you are paying to a company outside India.

2. When you have entered CVV/3D secure number and saved it on the merchant site.

3. Some merchants like Flipkart have a systems called Visa Safe Click which makes it possible to pay upto Rs.2000 without requiring OTP."

Q- 9. Sir it can be even ' @netflix ' even email spoof attack can be done sir. " Mr.Renganathan

Answer:- Mr. B.Kandasamy

"Email Spoofing is possible and that is one of the means used in Phishing. Phishing and spoofing are clearly different beneath the surface. One downloads malware to your computer or network, and the other tricks you into giving up sensitive financial information to a cyber-crook. Phishing is a method of retrieval, while spoofing is a means of delivery.

In addition to from email you can check for other signs of phishing by just reading the content of the email. "

Q- 10. In case of phishing when customer informs the bank about the fraud and issuing bank in turn informs the payment gateway to stop the payment. But the payment gateway supersedes the instruction and allows final settlement of the fraudulent transactions. How is the liability fixed? The customer or victim has all the relevant evidences like email from issuing bank to payment gateway..etc. Ms.Kajal Rajani

Answer:- Mr. B.Kandasamy

"1. One cannot lose money by doing a search online.

2. If you are referring to frauds done by people who pretend to be offering help or acting as call center, then it is always safe to avoid giving out confidential information over phone/email. Also do not download any software or app when unknown person asks you to do."

Q- 11. Why an online search may be the worst way to lose money? Helpline frauds.

Dr .K.V. Gangatharan

Answer:- Mr. B.Kandasamy

"1. One cannot lose money by doing a search online.

2. If you are referring to frauds done by people who pretend to be offering help or acting as call center, then it is always safe to avoid giving out confidential information over phone/email. Also do not download any software or app when unknown person asks you to do."

Q- 12. Kindly also explain how to investigate the crime. Ms.Sucheta

Answer:- Mr. B.Kandasamy

Crime Investigation is the exclusive subject of the Police. But Prevention of crime is the subject of every one.However I would like to place the followings:-

"It has to be investigated using different methods - digital techniques and human intelligence. It is a professional job by itself. Since you have asked, here are a few methods:

1. Trace the activity of the fraudster online using his email address.

2. Trace the IP address of the source of the email so we know the physical location and internet provider name.

3. Communicate with Bank and payment gateway provider to know the fraudster's bank account. That bank account will always be one of many middlemen of the fraudster.

4. Find out the source and owner of link or website that is in the email.

So now you know to some extent how cybercrime cases are cracked!. "

Q- 13. I guess every online transaction asks for CVV... is there an alternative where CVV need not be furnished!!? Ms.Sheena
Answer: - Mr. B.Kandasamy **"It is safe to provide your card details to sites like Amazon.** **Without that you will not be able to pay them. CVV is mandatory when doing online transactions."**
When i use amazon it asks for card details along with CVv. is it correct to furnish it? Mr.Manoharan
Answer:- Mr. B.Kandasamy **"It is safe to provide your card details to sites like Amazon.** **Without that you will not be able to pay them. CVV is mandatory when doing online transactions."**
Q-14 Is it safe in money transfer for any purchases online? like Gpay, paytm etc.? *Ms.Sheena*
Answer:- Mr. B.Kandasamy **It is "Digital India". It is safe to provide your card details to sites like Gpay, Paytm etc. It has become a part of our online activity.**
Q- 15. "I once ordered https://www.limeroad.com/ The delivery was getting delayed. So I was trying to contact LIMEROAD. During same period, I received a phone call from a man who told me that I should download the ""App"" he will provide. This ""App"" will let me track my consignments!! He had very bad English as well! Hilarious. But I wonder how they get information on who is contacting an authorized website regarding delay in delivery etc.!!? not to click is precaution but pl explain cure as well" Ms.Sheena

Answer:- Mr. B.Kandasamy

"Such frauds continue to happen. You should never download any software or app from unknown sources. There are chances that it is a coincidence or someone at lime road or its delivery partner has leaked your information to the fraudster. Such things do happen and many cases are reported. Always track your order only through the website your purchased. If you have downloaded any software or app which you think could be malicious, use free anti-virus app like Malware Bytes to scan your computer which will identify and prompt you to remove such software."

.....