Research Guru
Online Journal of Multidisciplinary Subjects (ISSN : 2349-266X)
Volume-13, Issue-2, September-2019
Impact Factor:4.081
www.researchguru.net

Critical Study of the Modus Operandi used by cyber criminals in cybercrimes related to Electronic Fund Transfer in India

Ms. Mamta Sanjay Karkar
(Research Scholar) 'Parvati Nivas', Shankar Tekri, Dandiya Bazar, Vadodara 390001, Gujarat

Abstract: *The Reserve Bank of India recently had launched an ombudsman scheme for Digital Transaction for the redressal of complaint against system participants. This is what the Reserve Bank has taken an initiative to provide the free of cost redressal mechanism for the grievances registered by the customers using various digital transactions through non-banking channels like mobile wallets or such similar other. For the transactions undertaken through the banking channels are supposed to be manage by the banking ombudsman. This prospective step has been taken by the Reserve Bank of India to combat the increasing cybercrimes related to Electronic Fund Transfer and provide the grievance redressal mechanism for the users. The cybercrimes are constantly increasing in the Indian e-banking system and there has been a great threat to the nation's economic growth. Another significant step taken by the State Bank of India for preventing increasing frauds through Debit Cards is the introduction of YONO Cash service. All these efforts are being taken on the national level to decrease the electronic fund transfer frauds through cybercrimes and save the customers, users of e-transaction, digital payment gateways etc. In spite of various precautionary steps by the Ministry of Information and Technology as well as CERT IN, the cyber criminals are adopting new modus operandi to make cybercrimes of Electronic Fund Transfer. This paper will particularly focus on the study of modus operandi used by cybercriminals in cybercrimes of Electronic Fund Transfer or Digital Transaction fraud. The study has based on the real incidents came into light through various information systems like newspapers, internet, research papers etc. The researcher has tried to identify certain common strategy used by the cybercriminals in the cybercrime related to Electronic Fund Transfer in India.*

Keyword: *Electronic Fund Transfer, Cybercrimes, Modus Operandi, Digital Payment, E-banking*

Introduction:

The establishment of National Payment Corporation (NPCI) was made in 2009 to enhance the development of electronic payments and digital transactions. Indian Banking system have introduced various electronic payment facilities like NEFT (National Electronic Fund Transfer), RTGS (Real Time Gross Settlement), IMPS (Immediate Payment Services), NACH (National Automated Clearing House), PPI (Prepaid Instrument) etc. in the e-banking system. At the same time the customers or internet users are using popular payment facilities through Paytm, mobile banking Apps, Wallets, Google payment services etc. Use of all these Applications or services are also termed as Internet Banking which refers to using Internet for banking services through such electronic gadget like Smartphone, PC, Laptop or tablet etc. Many services are also provided through Internet Banking like e-tax payment, payments of electric or telephone bills, balance inquiry, online share marketing, railway ticket booking, online food services etc.

As the use of online payments and money transaction has increased, the cyber criminals have came into action and online frauds are increased. Earlier the cyber criminals were using the technique of making phone calls to the customers and taking out information like Credit/Debit card number, account number and password, PIN etc. But in this study researcher has observed many other new techniques i.e. modus operandi has been adopted by the cyber criminals in the incidents of electronic fund transfer frauds. On the background of recent announcement of starting new Payment App by WhatsApp / Facebook, it is required that the users must become aware of the cybercrimes of digital payments or cybercrimes of Electronic Fund Transfer.

Materials and methods:

This research article has been written using the doctrinal method. The study of different literature in print and electronic media has done for the identification of the issue of various cybercrimes related to electronic fund transfer. The incidents published in daily newspapers, made viral through social media are the inspiration for observing such

modus operandi adopted by the cybercriminals in digital world.

Results: This study reveals the criminal behavior of the cybercriminals and loopholes in the cyber infrastructure. The lack of awareness in the customers and users of e-banking, digital payment services, users of online shopping, and other services is also the responsible factor for increasing cybercrimes in electronic fund transfer incidents.

The cybercrime cell or cybercrime branch has taken significant action in investigation as well as resolution of cybercrime cases.

The study of recent incidents of cybercrime related to Electronic Fund Transfer:

Incident 1: The new techniques or modus operandi adopted by cybercriminals in some major incidents of electronic money frauds are observed as follows. One of the big fraud of electronic fund transfer was recently came into news (published on 14/06/2019) when 3 Nigerians with other cybercriminals were arrested by the cyber cell team at Mumbai. The cyber cell ceased mobile phones, Passports, Dongle, Pen drive from the cybercriminals used in the cybercrime. The total amount of fraud declared by the cyber cell in this incident was 1.03 Crore rupees.

Modus Operandi: the Cyber Criminals used to send the link IG-ITDEFL to the customers and get bank details, mobile number with other credentials for data theft. Then cybercriminals successfully make Net banking for transferring the money. Four other criminals made available their bank accounts to the main cybercriminals for the purpose of withdrawing the amount from the banks. In this method the cybercriminals cheated the customers by sending fake link for IT refund and asking them to fill up the details for verification which were used to make money. The criminals also used to do such transaction in the late night so, the customer may not see the message of debited money.[1]

Incident 2: One person received a phone call offering attracted Gift on online purchase valued Rs. 599/- He purchased a purse, and he was told that he had won a phone as a gift of price Rs. 79,000/- After that the cybercriminal asked the customer to pay 10% amount of the gift for some procedure. Again he was asked to pay Rs. 599/- When the customer asked his money back, the criminals asked him to pay more Rs. 2000/- for refund, which he paid. Again the demand of Rs. 6660/- was put by the criminals. After this the customer complained at police station. In another same incident, a customer was cheated in the name of gift and bound him to make shopping of Rs. 5000/- paying through Google pay. The customer made the complaint after realizing that he had become the victim of fraud by cybercriminals.

Modus Operandi: in both the incidents the cybercriminal had tried to cheat the customers through giving offer of online purchasing for the attractive gift. And the customer himself has paid the money in the name of various tax or procedure fees for getting the gift. Ultimately after realizing that he is the victim of cybercrime, made the complaint.

In such incidents the customer must be aware that they should not pay money for any such fake gift calls or he should not give own credentials for any procedure. The cybercriminals have taken the benefit of mentality of customer to get free gift.

Incident 3 : in this incident a customer who was a constable of NDRF attempted to open a link for online booking of Gas cylinder. He was searching a gas agency for purchasing new connection and found a one address at Alkapuri Vadodara.[2] The constable made a phone call from his friend's phone. Form the other end the person asked to provide a phone number which is connected with Google pay and Bank. So the customer gave him his own bank account number which was salary account connected with Google pay. Then he received a link through a text message for gas booking form, which filled up and booked for gas connection. But he did not receive any message of successful form submitting, hence he tried again. After 15 minutes he received the message that Rs. 45400/- had been debited from his Bank of Baroda Account. Next he received the message of debit of Rs. 13830/- from his salary account. Then he realized that he had been victim of cybercrime related to electronic fund transfer by the cybercriminals.

Modus Operandi: the cybercriminals used to send a fake link for the online money fraud. The customers or mobile users are not aware of such link and they try to open it and get defrauded. Any customer, mobile or internet user should not open the link which is unknown or sent from unknown, unauthentic source.

Incident 4: One morning a ATM card holder received a message on his mobile that Rs. 50,000/- was debited from his account. He came to know that his ATM card has been lost from his pocket. And total five transactions were done in the night during 1.30 am to 2.00. The victim had not provided his PIN to anyone, and still the money had been debited. He made the complaint to the police station.[3]

Modus Operandi: in this incident it is clear that the transaction was done using PIN of the ATM

card, may be manually or electronically by the criminal and not by the real card owner. The criminal might have used the PIN or OPT for such transaction after hacking such data from previous online transaction.

Incident 5: Use of fake account on OLX. In another incident one criminal put an offer to sale a white Desire car on OLX on date 10-01-2018to 27-10-2018. One person from Rajkot contacted on the given number in the advertisement. The criminal asked the purchaser to transfer Rs. 21 thousand in Paytm wallet and informed to see the goods (car) in Rajkot. When the victim reached to Rajkot, he came to know that he has been cheated by fake offer. After his complaint to cybercrime cell, the criminals was arrested from Hariyana. [4]

Modus Operandi: In such incident the criminal has used the strategy of fake online sale by the use of website OLX. He was trying to show that the vehicle is of Army Cantonment and used Army I-card, Photo in uniform, canteen card so the customer should believe him.

Incident 6: In one more news the cybercrime came to know in the form of using fake Facebook account of a women by the criminals. The complainant registered that cybercriminals prepared a fake Facebook account in the name of a women and made friendship with the victim (complainant).[5] Then the criminal discussed with victim that she is making research on Cancer medicines and need Narcozin raw oil, and asked him to do business of this product which will be much beneficial. The victim got trapped in her offer and then the criminal purchased the same product from victim through (her own) fake customers. Then victim was given a big purchase order and also asked to pay Rs. 65 lakh in different bank accounts. When the victim was realized that he had been cheated by the criminals he made the complaint in cyber cell. Seven cybercriminals were tracked by the cyber cell including 2 Nigerian persons.

Modus Operandi: In the investigation it was observed by the cyber cell that the criminals had used this modus operandi to cheat the people of Gujarat, Maharashtra, Tamil Nadu and Andhra Pradesh also. The gang was used to make fake account of woman and offers business deal with various businessmen, for the business of raw oil /raw material. They used fake customers or purchasers and inspector of goods to achieve the faith of such victim. The investigation is in procedure.

Incident 7: In another case the cybercriminals from Delhi Call center made online fraud by electronic fund transfer of the victim through Job career website. One female, resident of Vadodara [6] applied for the Job Career Website in search of job. She applied through online form in which the criminals also asked her to fill up debit card details for a very small amount of Rs. 49/-. And then the criminals made three transactions for debiting Rs. 19 thousands from her accounts. The victim made the complaint to cyber cell. In the cyber cell investigation the team detected the cybercriminal gang from Delhi who were running a call center at Delhi and cheating such job seekers through online website.

Modus Operandi: the cybercriminals in this case used the psychological effect to make cyber fraud of the fund transfer. The young candidates are always use online search for the employment. The criminals attempted to target such young job seekers to make the fraud of electronic fund transfer. The cyber cell investigated that in this call center fraud total 18 young candidates were become victim of the cybercrime of electronic fund fraud through misuse of their debit or credit card details.

Incident 8: In a new type of cybercrime related to electronic transaction of money, different mode has been came into light. A customer (victim) received a computerised voice call (fake) telling him that the caller is speaking from a reputed bank and confirming whether he has done a transaction of Rs. 3999/- from his account just now; if yes press 1 and if not done press 8. The victim hadn't done any such transaction, so he pressed 8 as per instructions, Rs. 20299/- was deducted from his account within 5 seconds. He immediately blocked his account from bank. In this case the victim has not revealed any of his details to any one, still his money was lost due to cybercrime of electronic fund transfer. [7]

Modus Operandi: In this matter the cyber criminals has used a complete technological set up to achieve the motive. The cyber criminals has advanced voice skimmer device connected with the laptop. The software installed in the set up make voice recording with the help of voice skimmer device and laptop. As the victim press the number, his complete search history of the mobile, either Google search or any App search is moved to the Laptop connected with the voice device. This history can be accessed with the help of malware coding and command line. In this history, the passwords of banking App, social media history, and all data is converted in the graphics in the laptop and cyber criminals can get the data which they have targeted. In this way some technically

advanced cyber criminals are taking the advantage of mobile user's data and search history to make the cybercrime of electronic fund transfer.

The cyber expert Mayur Bhusavalkar explained in one interview on cybercrime that the cybercriminal gang try to attract the targeted victim to act in specific way by offering various schemes, or make message like preapproval loan has been passed, and send the link on the mobile or PC or Laptop. Once the victim open such link and fills up details, any amount may be debited from his account.

Conclusion: Cyber criminals are discovering new and fresh modus operandi for the cybercrime of electronic fund transfer through mobile and computer taking advantage of the user's mentality of online transactions, shopping sites and advanced technology. The researcher has observed that the causative factors behind such cybercrime incidents particularly of electronic fund transfer through banks, ATM cards, mobile App etc. includes lack of awareness of the users for the new technology, hasty use of the online shopping sites and getting trapped in the attraction of gifts, less price, sale etc.

The critical study of the modus operandi used in various incidents discussed in the paper shows that the risk of cybercrimes related to the electronic fund transfer has been increased. The users or account holders should be precautious to avoid such cybercrime by taking following steps :

- The users should not open any email received from unknown source with attachments.
- Do not open any link which is not authentic and ask to fill up personal information and credentials.
- Users should always delete the history in the browser, remove cookies etc.
- Cut off the unwanted or unknown call.
- Do not save the password in mobile apps which are used for electronic transaction of the money.
- Users should not reveal any information to the person who says that he is calling from the bank.
- Shopping sites or online sale sites should be used carefully and payment should not be done before the delivery of the goods.
- Card holders should not use the card in ATM's when any strange person is inside,
- Users should be aware of such criminal minded persons who are offering job without any pre-advertise and authentic address directly online.

The cybercrime can be detected with the help of the cyber experts and cyber cell. But the users of new technology can help to prevent it from the root if they become aware of the risks hidden in it. This new patterns of technical crimes can be combatted by the knowledge, precaution and awareness in the users. The Information Technology Act and National Cyber Policy, as well as the cyber infrastructure are helpful for the stringent provision to prevent and punish cybercrimes.

References:

[1] published in newspaper dtd. 14/06/2019
[2] published in newspaper dtd. 9/07/2019
[3] published in newspaper dtd. 29/01/2019
[4] published in newspaper dtd. 25/02/2019
[5] published in newspaper dtd. 18-03-2019
[6] published in newspaper dtd. 31/3/2019
[7] published in newspaper dtd. 30/06/2019