Cyber Financial Fraud's Threat: Avoid the Virtual Conman's Net!

'Jamtara' a Netflix series is watched and liked by many of us. The series highlights the rising trend of online cyber fraud in India and the challenges faced by the law enforcement agencies in dealing with it. Fraud has existed since time immemorial and has a tendency of the human mind to gain an undue advantage over another. With advancement of technology and monetary transactions online, cyber financial frauds have become very common. In this article, we explore recent examples of cyber financial frauds and the reporting mechanism available to the citizens. [1]

The term cyber financial fraud is not defined under the laws but is generally understood to mean certain online criminal activities that involves using technology to steal money or sensitive financial information from individuals or organizations. It is growing problem in India, with fraudsters using a range of tactics like phishing, usage of online sale platforms, usage of scammed QR codes etc., to steal money from individuals and organisations across various sectors.

[1]

. The effect of cyber financial fraud is significant in India as the traditional literacy and digital literacy is very slow in India.
In an RBI circular , The RBI has classified financial fraud into various categories such as: [2]

- Misappropriation and Criminal Breach of Trust,
- Fraudulent Encashment through forged instruments,
- manipulation of books of account or through fictitious accounts and conversion of property,
- unauthorized credit facility extended for reward or illegal gratification,
- cheating and forgery, fraudulent transactions involving foreign exchange,
- or any other type of fraud not coming or specified as above.

1. **Phishing**

Phishing is a literal word play on fishing, where a bait is dangled in the hope that a fish would bite and get hooked. Phishing is a type of cyber-attack that involves sending fraudulent emails or messages to trick people into divulging their personal or financial information, such as password, credit card details or bank details. In India, phishing scams can take various forms, such as impersonating popular brands, government agencies, creating fake social media profiles.
Nasscom v. Ajay Sood ,. The defendants in this case, impersonated NASSCOM, a leading software association. The Delhi High Court took a note of developing trends in commission of fraud including phishing attacks online and concluded that it would constitute a criminal offence. It was for the first time the term “Phishing” was defined in in this case as - "Phishing is a form of internet fraud. [3]
. In. In case of ‘Phishing’, a person pretending to be a legitimate association such as a bank or an insurance company in order to extract personal data from a user such as access codes, passwords etc. which are then used to his own advantage, [4]

2. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD28A4C421E7F7724C07B38E3C6207F3548E.PDF
[119 (2005) DLT 596
3. [119 (2005) DLT 596]
4. https://indiankanoon.org/doc/1804384/

data from a user such as access codes, passwords etc. which are then used to his own advantage, misrepresents on the identity of the legitimate party".

Personal information obtained by misrepresenting the legitimate party's identity is frequently exploited to the benefit of the collecting party. The court further defined it as "a mis-representation made in the course of trade, leading to confusion as to the source and origin of the email, causing immense harm, not only to the consumer, but also to the person whose name, identity, or password is misused."

Instances where people were lured through Phishing:

U. P lawyer duped Rs. 40,000:

A High court lawyer has been duped of Rs. 40,000 by a miscreant by using the name of his friend who is the Senior Superintendent of Police (SSP) of Bareilly. In his complaint filed before Aliganj police station, Mr. XYZ of sector C of Aliganj said he got a message on Facebook messenger from a man who introduced himself as CRPF official at Kanpur headquarters. "The man further said he got my mobile number from our common friend, SSP Bareilly Akhilesh Chaurasia who asked him to contact me to get his issue resolved,". The miscreant said he had been transferred to Jammu and Kashmir and he wanted to get his household articles sold for Rs 40,000. The victim agreed to help the miscreant and transferred the money to a bank account of one Kartikeya. The Complainant waited for the items to be delivered to his address, but it never came. He thereafter called up SSP Bareilly who was ignorant about the man and his nefarious scheme [5]

Women lost 7 lakhs after activating credit card:

In a recently reported case by Times Now, a woman from Panvel, Mumbai fell victim to an online scammer who duped her on the pretext of offering a credit card and a free Android phone. According to the report, the 40 years old women received a call from "Mr. XYZ" who introduced himself as a bank employee and offered her a new credit card and membership of a sports club in the city. Falling for his offer, the woman agreed to get the new credit card. She even shared her personal details including her Aadhaar card with the fraudster to initiate the process. Furthermore, the scammer, said that the credit card can only be activated using an Android smartphone. Since the woman was using an iPhone, he asked her to change the device with the new phone which he will be sending. The woman agreed to use the new phone and shared her home address at which she could receive the new Android phone. After sharing all the details, the woman received the new Android smartphone on the same day of the call. [6]

5. https://cybercrime.gov.in/Webform/dailyDigest.aspx
6. https://cybercrime.gov.in/Webform/dailyDigest.aspx

Reportedly, the phone has two pre-installed apps -DOT Secure and Secure Envoy Authenticator. After receiving the phone, Mr. XYZ asked the woman to insert her SIM card into the new phone and follow the instructions to complete the activation process of the credit card.

The transaction was from a jewellery shop in Bangalore. After getting messages about the unauthorised transactions, the woman realised she was scammed. However, since the banks were closed on that day, she was unable to verify the transactions and reported the case of fraud the next day. She approached the bank and later filed a case with the police while the case is under investigation.

Fraud using online sales platforms.

Fraudsters pose as buyers and sellers on popular online marketplaces like Quikr and OLX and trick people into sending money or goods without completing the transaction. Recent Fraudsters modus operandi is that they impersonate themselves to be Army personnel to trick people to believe them. As a seller they post second hand good stuff online on very cheap rate to attract people and once they are approached by the buyer, they convince them with their fake Army Id's about their authenticity and trick them to pay the advance amount of the product. Once the payment is done, they delete their listing from such websites.Recently in Mumbai Two accused cheated multiple victims of over Rs. 10 lakhs through OLX scam. The police have registered a case against two persons who allegedly scammed multiple victims by taking money into their accounts on the pretext of buying and selling materials from OLX. The scam reportedly took place from July 7, 2022, till recently. One of the victims, filed a complaint stating that he and others were contacted by unknown individuals from different numbers who induced them to transfer money to their accounts in exchange for materials from OLX. The victim transferred Rs. 46,300 from his account to the accused's account, while others transferred a total of Rs.1,32,300 from various bank accounts. The victims were cheated of a total of Rs. 1,78,600. [7]

QR Code Scam

QR code Scam has become a growing concern in India, as the use of digital payment methods has increased in recent years. QR codes, which are two-dimensional barcodes that can be scanned using a smartphone have become a popular target for cybercriminals in recent years. There have been reports that fraudsters create fake QR code and use them to steal money from people's bank accounts.

7. https://timesofindia.indiatimes.com/city/hyderabad/olx-fraud-conmen-pose-as-army-officers-to-extract-funds/articleshow/74165444.cms

.One type of QR code scam is known as QR code phishing. This is where a criminal creates a fake QR code that directs the user to a phishing website designed to look like a legitimate site. Once the victim enters their login credentials or other sensitive information on fake website, the criminal can use that information to steal money or commit other fraud.

Another common QR code scam is when the fraudster sends the QR Code to the victim to receive money. In this type of scam, the criminal asks the receiver to scan the QR code and enter the amount to be received and once the receiver enters the OTP the amount is debited from the receiver's account instead of Sender.

Man selling cupboard on OLX; loses Rs. 8 lakhs : In this case, a 44-year-old man resident of Nerul, Navi Mumbai working in Dubai was duped of Rs.8 lakhs by fraudster posing Army personnel. The Complainant had posted an Advertisement to sell cupboard on OLX platform. The conman contacted complainant for buying his cupboard for Rs.7000/-. Under the pretext of making an online payment the conman made him scan a QR code sent on his WhatsApp. . Instead of crediting Rs.7000/- to complainant's bank account, Rs.96,000/- got debited from his account. When the complainant questioned the conman, he claimed that it was technical error. For refunding the amount the complainant was asked to contact Army's technical expert. To gain the trust of the Complainant the conman sent his photograph in Army uniform on WhatsApp. Thereafter the Complainant was contacted by conman's aid, and he sent him an account number and made him add as beneficiary for crediting Rs. 96,000/- back to his bank account. Once the beneficiary was added the Complainant started getting several bank alerts through texts stating that transaction of Rs. 2 lakhs and 5 lakhs were transferred from his account to the new beneficiary. The Complainant blocked the account and made Police Complaint in Nerul Police Station. After recording statements an FIR was registered under Section 419, 420 of IPC along with Section 66C and 66D of IT act, 2000. [8]

Understanding Cyber Financial Fraud

All above online crimes will come within the purview of definition of Phishing. The online financial fraud usually manifests in two ways:

1) Impersonation of legitimate person; and

2) theft of data.

In Cyber Financial fraud or Phishing an individual impersonates another in the virtual world to gain access to sensitive data and it has been found to be one of the least expensive methods for criminals. Given the lack of knowledge a victim has of what needs to be done when dealing with such financial frauds, this article is an attempt to understand cyber financial fraud and laws dealing with in India.

8. https://timesofindia.indiatimes.com/city/navi-mumbai/navi-mumbai-nerul-man-seeking-buyer-to-sell-cupboard-on-olx-loses-rs-8-lakh-to-cyber-frauds/articleshow/886445

Cyber Financial Fraud is subject to the provisions of Information Technology Act, 2000 (“IT Act”) as there is a theft of sensitive data from virtual world and hence it falls within the ambit of cybercrime. Section 66 , 66C and 66D of the IT Act and Section 416, 417, 418, 419, 420 of Indian Penal Code, 1860 (IPC) deals with the financial cybercrime.

CBI v. Arif Azim In this case, a complaint was filed by Sony India Ltd, which runs a website named www.sony.sambandh.com. This website enables NRI to purchase and send products after making online payment to their friends and relatives in India. The Accused in this case had made payment via a credit card owned by an American citizen to deliver a television set and headphones to a person named Arif Azim who resides in Noida. Later when all the formalities and delivery were done the credit card company informed Sony that the card user is denying such payment and Sony lodged a complaint in CBI regarding the fraud. Later it was found that Arif Azim an employee of a call center acquired the detail of the card user and used to order the products by the detail of the card. A complaint was registered under Sections 418, 419, and 420 of the Indian Penal Code, 1860. The investigations concluded that Arif Azim while working at a call centre in Noida, got access to the credit card details of Barbara Campa which he misused.
The Court convicted Arif Azim but being a young boy and a first-time convict, the Court has taken lenient approach towards him. The Court released the convicted person on probation for 1 year. This was one among the landmark cases of Cyber Law because it displayed that the Indian Penal Code, 1860 can be an effective legislation to rely on when the IT Act is not exhaustive. [12]

Penalties for Cyber Financial Fraud.

9.This deals with hacking with computer system
10. whoever, fraudulently or dishonestly make use of electronic signature, password, or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.”
11. According to this provision “whoever, by means for any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.”
12. https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf

Section 66 C of IT Act	Section 66 D of IT Act	Section 419 of IPC	Section 420 of IPC
•Identity theft is punishable with imprisonment upto 3 years and fine which may extend to 1 lakh	•Cheating by personation using computer resource is punishable with imprisonment upto 3 years and fine which may extend to 1 lakh	•Cheating by personation is punishable with imprisonment upto 3 years or with fine or both.	•Cheating and dishonestly inducing delivery of property is punishable with imprisonment upto 7 years and shall also be liable to fine.

Additionally, the provision under Section 81 of the Act is an obstante clause whereby the provisions of the IT Act has overriding effect over all other provisions within the existing law. However, it is also important to note that, pursuant to Section 77B of the IT Act (Amendments 2008), offence under the above-mentioned provisions of IT Act is bailable. This is based on the inability to determine with certainty, who is the perpetrator behind the crime. In this mode of the crime the fraudsters hide their identity which results in situations wherein an innocent person can get convicted for a crime that they have never committed; this created the need to make provisions for bail under Section 77B of IT Act.

The biggest challenge while investigating the cyber financial fraud is to track the fraudsters as they operate online using fake identity and commit this offence sitting in different city and State. Fraudsters using mobile numbers and bank account are registered in the name of innocent person who are not even aware of their identity being stolen so even if police are able to track the mobile number owner its mostly doesn't lead to the actual culprit.

Crucial remedy through the eyes of RBI:

Apart from IT Act, The Reserve Bank of India ("RBI") has recognized the issue of cyber financial fraud and has issued guidelines and have also introduced a Master Circular titled "Master Directions on Fraud- Classification and Reporting by Commercial Banks and select FIs" (hereinafter referred to "Circular") on July 01, 2016. [13]

In addition to the above guidelines, a scheme namely I4C (Indian Cyber Crime Co-ordination Centre) has been formulated by Ministry of Home Affairs for reporting Cyber Financial Fraud.

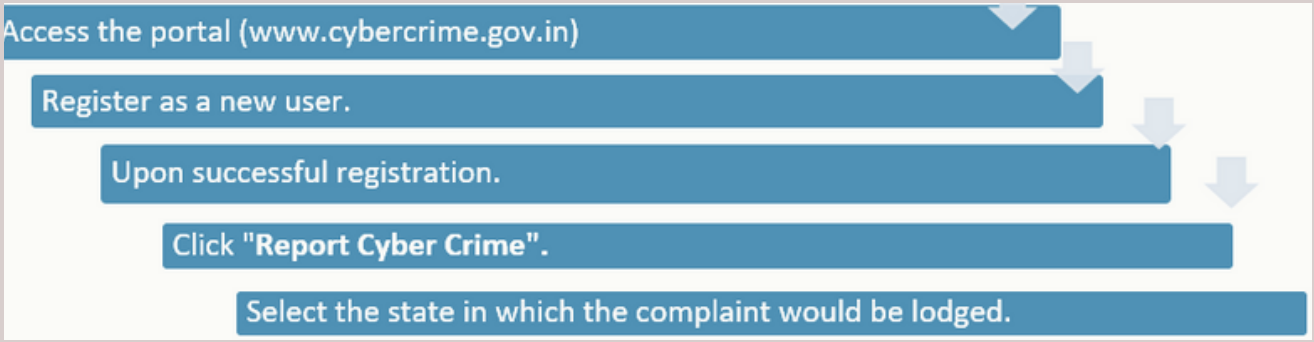
13. https://m.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=10477

Under this scheme various centres and units for investigation and identification of cybercrime were launched such as National Cybercrime Threat Analytics Unit (TAU), National Cybercrime Reporting, Platform for Joint Cybercrime Investigation Team, National Cybercrime Forensic Laboratory (NCFL) Ecosystem, National Cybercrime Training Centre (NCTC), Cybercrime Ecosystem Management Unit, and National Cyber Crime Research and Innovation Centre. [14]

In case a cyber-financial fraud is committed, then the victim can lodge a formal complaint on the National Cyber Crime Reporting Portal (www.cybercrime.gov.in).

Procedure for lodging a complaint on National Cyber Crime Reporting Portal:

In case a financial cyber fraud takes place, then the victim can register their complaint on cybercrime website.



As per RBI Circular on "Frauds: Classification and Reporting" the complaint is marked to the cyber cell and accordingly an FIR is also lodged at police station where the offence is alleged to have been committed. It is pertinent to note that there is no legislation which specifically provides for cyber financial fraud as a separate class of offence. However, as per previous RBI Circulars, in such cases, the provisions of Indian Penal Code would be invoked while registering such cases.

Whenever financial fraud is committed either through online mode or otherwise, time is of the utmost essence, and the RBI guidelines require the person to report the same as soon as possible. It is settled that the law favours the vigilant and does not come to rescue the one who slumbers upon his rights. If the victim quickly reports the commission of fraud, then as per I4C Scheme, the chances of recovery of duped amoun are higher. In cyber financial fraud, it is the cyber cell of the police which investigates such cases.

Conclusion

The ways to commit Cyber Financial Fraud is constantly evolving into new territories. Once details of a modus become a common knowledge, cybercriminals find a new way to apply their skills.

14. https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme

Even though there are provisions to deal with cyber financial frauds, but still cyber financial frauds are increasing as people are not aware of such frauds and lack information to deal with such frauds like informing the bank and filing complaints in cybercrime portal. Sometimes when victims approach the police for such frauds, the police fail to register the complaint which delays the process of investigation and give enough time to the fraudsters to commit further crimes. On 4th March 2022 in Shiv Kumar vs. State of Bihar the Patna High Court issued a show cause notice to the officer for not registering a case of Ms. Kanchan Jha (complainant) who suffered a monetary loss of Rs.21 Lakhs through a cyber financial fraud where money was withdrawn illegally via two concerned banks. The Court after acknowledging the facts of the case asked the Economic Offences Unit to investigate the case further and directed complainant to get FIR registered with Economic Offences Unit by next day.
To protect oneself from cyber financial fraud, it's important to be cautious while scanning code from sources you don't trust. Check of any signs of tampering or suspicious activity, such as QR code that looks different than usual or leads to an unexpected website. Always verify the legitimacy of any requests for payment or sensitive information and use two-factor authentication and other security measures whenever possible. It's also a good idea to keep your devices and software up to date with the latest security and to use antivirus and anti-malware software. [15]
There are certain precautions mentioned as per RBI's guidelines which can surely help to avoid such Cyber financial frauds. [16]

• Do's

- Regularly check SMS / emails to ensure that no OTP is generated without your prior knowledge.
- Exercise due care and vigilance while providing KYC and other personal documents, including the National Automated Clearing House (NACH) form for loan sanction / availing of credit facility from any entity, especially individuals posing to be representatives of these entities.
- Avoid saving card details on websites / devices / public laptop / desktops.
- Change passwords at regular intervals.
- Log out of the internet banking session immediately after usage.

· Don'ts

- Never share OTP / PIN / personal details, etc., in any form with anyone, including your own friends and family members.
- Never open / respond to emails from unknown sources as these may contain suspicious attachment or phishing links.

[15] Criminal Miscellaneous No.38807 Of 2020
[16] https://cms.rbi.org.in/

Keep the PIN (Personal Identification Number), password, and credit or debit card number, CVV (Card Verification Value), etc., private and do not share the confidential financial information with banks/ financial institutions, friends or even family members.
Do not store secure credentials / bank passwords, etc., in emails.
Avoid using public terminals (viz. cyber cafe, etc.) for financial transactions.
For any feedback or response on this article, the author can be reached on pranav.mane@ynzgroup.co.in, suhas.joshi@ynzgroup.co.in , priya.shahdeo@ynzgroup.co.in

Suhas Joshi is experienced in Litigation. By qualification he is Bachelor of Commerce and Bachelor of Law from Mumbai University.

Pranav Mane is an associate at YNZ Legal. By qualification he is Bachelor of commerce and Bachelor of Law from Mumbai University.

Priya Shahdeo is an associate at YNZ Legal. By qualification she is Bachelor of Arts and Bachelor of Law (B.A.LLB) from Bharti Vidyapeeth University. She is also member of Bar Council of Delhi.