DEEPSTRAT
STRATEGY . POLICY . ACTION

The Dialogue™
INFORM ENGAGE IDEATE

TACKLING RETAIL FINANCIAL CYBER CRIMES IN INDIA

Tools | Techniques | Tactics | Tests

An Ethnographic Study

CHANDER MOHAN (IPS)
SAIKAT DATTA
ANAND VENKATANARAYANAN
KAZIM RIZVI

Authors

Mr. Chander Mohan, IPS

Mr. Chander Mohan is from the 2015 batch, Haryana Cadre of the Indian Police Service. He is also an electrical engineer from the Indian Institute of Technology, Delhi. He is currently posted as Superintendent of Police, Mahendergarh district, Haryana.

Mr. Saikat Datta

Mr. Saikat Datta is the founding partner at DeepStrat and Strategic Advisor with The Dialogue and NullCon. He is an award-winning journalist, tech policy and security specialist. His expertise lies around strategic communications, media, public policy, de-risking strategies, government relations, risk assessment and mitigation, security affairs, and threat intelligence.

Mr. Anand Venkatanarayanan

Mr. Anand Venkatanarayanan is a cyber security and privacy researcher. He also dabbles in financial modelling. He is a public interest technologist and has written extensively about cyber security issues in several publications.

Mr. Kazim Rizvi

Mr. Kazim Rizvi is a public-policy entrepreneur and founder of leading policy think tank, The Dialogue and also a co-founder at Deepstrat LLP. A lawyer by training, Kazim envisages to drive change in India through the medium of policy and research.

Table of Contents

NOTE: All views expressed in this study are personal and in no way reflect the views of the institutions the authors are associated with. This is an independent study with an attempt to track trends and issues related to the investigation of financial cyber crimes based on a limited data set for a study carried out in a defined time period.

I. SUMMARY OF RECOMMENDATIONS

a) There is a need for a dedicated effort to collect structured empirical data on cyber payment frauds to assess the magnitude of the problem countrywide.

b) A regulator such as the Reserve Bank of India needs to evolve safety features and processes of all stakeholders in the digital payments' ecosystem for greater harmonization and safety of users. This will also aid LEAs in reducing their effort to carry out successful investigations of financial cyber-crimes.

c) Organizations like the NPCI or the proposed NUE must have a mechanism for identifying and tracking transactions linked to financial cyber-crimes to ensure speedy tracking and resolution for LEAs.

d) A data sharing standard across all stakeholders to ensure timely access to law enforcement for investigations.

e) Cyber-crimes are complex cases from an investigative point of view and therefore the provisions to make these cases compoundable should be reviewed.

f) The IT Act under section 78 mandates that only an Inspector or above rank of police can investigate cases registered under section 66 of the law. This needs to be reviewed to increase the pool of investigators available in the small states.

g) Cyber-crimes need regular and specialized training capsules for LEAs from information security researchers and academicians to stay abreast of the latest techniques deployed to commit frauds.

h) The KYC norms do not work for investigators and LEAs since multiple cases have been found with inadequate or fraudulent credentials. These need to be reviewed and strengthened.

i) Regular checks of sample KYCs can be carried out at regular intervals as an oversight mechanism with penalties on Telecom/Bank officials for irregular entries.

j) States where cyber-crimes originate can appoint a dedicated police officer to liaison with other states to enable investigation, arrests and prosecution and coordinate with the Union Ministry of Home Affairs, India Cyber Crime Coordination Centre (I4C) and Regional Cyber Crime Coordination Centre.

II. FOREWORD

Nandkumar Saravade IPS (Retd)

We happen to live in exciting times. The pace of change around us is rapid and accelerating. The massive use of technology in delivering financial services has already given a fillip to the availability, ease, and customer delight in paying and receiving money. Governments can transfer subsidies seamlessly, avoiding notorious leakages of past. More innovations are on the way, which will make the dream of financial inclusion a reality in a matter of a few years. However, as we know, where there is money, fraudsters follow. It appears that in the fog of change, there are many innocent wayfarers who are being waylaid, causing potential loss of trust, and erosion of the true potential to achieve the dream.

The current study, of payment frauds reported in south Haryana, is a tremendous contribution by the authors, given the shortage of field studies relating to policing in India. With its ethnographic approach, it provides the much-needed granular view from the trenches, that will inform making of the right strategy immensely. I congratulate the participants, especially the police officers, without whose wholehearted support, despite their overworked and stressful schedules, the project would have been stillborn. I hope this marks a happy trend where key stakeholders can collaborate with police to identify problems early and work towards creating solutions. The recommendations of the study would be very useful to the policy makers in central and state governments, police heads, the Reserve Bank of India, National Payment Corporation of India, and the payment industry in general.

With this good beginning, I would urge even more ambitious approaches. The traditional method of a complainant having to present himself at a police station to file an FIR is a BIG deterrence in capturing the crime trends. In payments frauds, the amounts involved are small, which, in a way, explains the reluctance of the police to register/investigate, given the all-India nature of the crime.

Bold steps like the following can really make a dent in the problem of dealing with financial frauds:

- Since it is not cost-effective to investigate all payment frauds, the Code of Criminal Procedure (CrPC) to create a category of crimes to be registered, but not investigated. As an interim measure, this can be done administratively by the state DGPs, prescribing a threshold of financial loss. This will enable police to go after the organized gangs, rather than doing futile paperwork on thousands of cases, which clog the criminal justice system.

- Pull data from the payment systems (UPI/NFS) to ensure stepped up registration. Identify organized crime patterns and go after the masterminds.

- Separate the investigative process into discrete steps to lighten the burden of the frontline staff.
- Create a strong backend unit for data processing to standardize documentation and file prosecutions speedily.
- Enable mechanisms of inter-state investigation, without the investigator necessarily traveling all the over the country, by creating parallel workflows which can be handled by the local police stations, with clear turn-around times.

The redoubtable Professor Einstein once said, "We cannot solve our problems with the same thinking we used when we created them." As we innovate in financial services, we need to envision similar transformative changes in the response mechanism, viz police investigators, to combat financial fraud, which has become high-volume, rapidly-mutating and run by organized-criminals, against whom most ordinary citizens do not stand a chance.

Nandkumar Saravade,
IPS (Retd)

Place: Mumbai
Date: 14th February,2022

Mr. Saravade was the Founding CEO of Reserve Bank Information Technology Pvt. Ltd. (ReBIT). ReBIT was set up in 2016 as a fully-owned subsidiary of RBI for technology management and cyber security for RBI's systems and the Indian banking sector. He is currently Strategic Adviser, Deepstrat.

1. EXECUTIVE SUMMARY

The rise in digital payments and the availability of multiple digital services has seen a proportional rise in financial cyber-crimes in India. Financial cyber-crimes have also emerged as one of the most pernicious side effects of the covid pandemic, as digital transactions have increased. For instance, the total number of recorded cyber-crimes, in the year 2019, was 44,546[1] , while the figure was 27,248 in 2018, and 21,796 in 2017, indicating an increasing trend even before the pandemic set in. ATM, Online Banking and OTP Frauds were 2066, 2091 and 549 cases, respectively, amounting to a total of 4706 out of the 44,546 cases. These frauds contributed to nearly 10.56% of the cyber-crime cases.

Worryingly, there seems to be a discrepancy between multiple authorities on the number of financial cyber-crimes that have taken place in India[2] . While the Reserve Bank of India (RBI) contends that there were 69,410 cases[3] , the National Crime Records Bureau (NCRB) has recorded 30,142 cases for the same period. A report published on the news website, The Ken, claims a much higher number of financial cyber-crime cases using anecdotal data[4].

Other reports[5] indicate that after the pandemic set in, in a single city-state of Delhi, the total number of cyber-crime related cases filed was 32,896, from January 2020 to December 2020 alone, an approximately 8-fold jump in cyber frauds from the previous year's number across all states and union territories. What is unclear from these two sources is the money defrauded by the scamsters from the victims and the evolution of the modus operandi and other contextual information such as why these crimes are exploding, the resolution rate and impediments faced by investigators in solving them.

The lack of this information is a blind spot for policy makers because all they see and hear is the ever-increasing adoption of digital financial transactions[6] , but not the growth limiting problems that increase in fraud poses. For instance, it is unclear which segment of the population is more vulnerable to payment frauds, and what remedial measures must be taken to mitigate the vulnerability because of lack of granular data, categorized across various modus operandi.

The lack of data on payment frauds, also leads policy makers to ignore investment on grievance redressal and instead focus on growing the volume of digital transactions, by reducing the cost of digital transactions, through approaches such as the Zero MDR (Merchant Discount Rate)[7] . But it has been clear to other successful market players that bringing down fraud volumes, sets them up for long term success[8] , by increasing trust among customers and businesses.

The purpose of this study is to try to fill this existing gap, by taking both a qualitative and quantitative approach to understand how payment frauds have evolved from the pandemic year of 2020.

---

[1]Ministry of Home Affairs. Crime in India 2019, Volume 2. National Crime records Bureau. [Online] 2020. https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%202.pdf

[2]Nandkumar Sarvade, Tackling UPI Frauds: Security by Design is the answer, [Online], 2022, https://www.moneylife.in/article/tackling-upi-frauds-security-by-design-is-the-answer/66298.html

[3]Govt. Of India, Ministry of Finance, UQ No 1188, 2021, [Online], http://164.100.24.220/loksabhaquestions/annex/177/AU1188.pdf

[4]Arundhati Ramanathan, The UPI Frauds undermining India's payments Fairy Tale, [Online], 2022, https://the-ken.com/story/the-upi-frauds-undermining-indias-payments-fairytale/

[5]Haider, Tanseem. Delhi saw maximum cybercrimes during Covid-induced lockdown. [Online] India Today, December 20, 2020. https://www.indiatoday.in/cities/delhi/story/delhi-saw-maximum-cybercrimes-during-covid-induced-lockdown-1751246-2020-12-20

[6]PRICE. Digital Payments well entrenched in Indian households across income groups, reveals PRICE and NPCI pan India Survey. [Online] January 14, 2021. https://www.npci.org.in/PDF/npci/press-releases/2021/NPCI-Press-Release-Digital-Payments-well-entrenched-in-Indian-household.pdf

[7]Hindu Business Line. Zero MDR: FinMin says no to banks' compensation plea. [Online] January 07, 2020. https://www.thehindubusinessline.com/money-and-banking/zero-mdr-finmin-says-no-to-banks-compensation-plea/article30506416.ece

[8] Allison, Chelsea. PayPal's history of fighting fraud. [Online] March 01, 2019. https://fin.plaid.com/articles/paypals-history-of-fighting-fraud/

2. BACKGROUND

Payment frauds are essentially extraction (taking out) of money from a payment instrument by either technical means (hacking) or through social engineering by tricking the owner. In both these approaches, the idea of the scammer is to release the locks, for which the holder possesses the keys, which allow extraction of money to some other payment instrument in their control.

While digitization has indeed changed payment transactions and how they are conducted, some conventional methods from an earlier era persist. For instance, if one might compare a donation box which has an open slot for anyone to drop money with a lock and key for taking it out, with a bank account some similarities still exist. All one needs to deposit money in it is a public identifier such as a bank code and an account number, while to take money from it requires possession and control of secrets such as username, password, physical cheque paper, ATM Cards, etc.

Three common techniques to manage the locks to take money out of payment instruments are:

- What you know – A secret such as a static password, personal identification number (PIN) or a dynamic secret with an expiry such as Time-based One-Time Passwords (OTP).
- What you have – Possession of a device (USB key, hardware token), a smart card (ATM Card), a cheque book (physical paper).
- What you are – A unique identifier that identifies the person such as fingerprint, facial identifier, palm scan, or even a signature.

The table below lists how these techniques are implemented while designing locks that govern money transfer across various payment instruments.

Lock Mechanism	What you are	What you have	What you know
Cheque	Signature (by hand)	Cheque Book (Pre-printed Paper)	N/A
Internet Access	Username	Soft (or Hard) Token device (if implemented)	Static / Dynamic password
ATM Withdrawal	N/A	ATM Card	PIN (Personal Identification number)
Physical Card Transaction	N/A	Credit / Debit Card	PIN (only for high value transactions)
Internet Card Transaction	N/A	Credit / Debit Card	CVV (Card Verification Value) and OTP (not applicable for international transactions)
Mobile Access	N/A	Mobile Device	OTP

Micro ATM (Aadhaar Payment)	Aadhaar Number + Biometric	N/A	N/A
UPI (Unified Payment Interface) Apps		Mobile Phone	PIN (Mobile)

Table 1. Protective Measures Against Payment Frauds

Scamsters typically attempt to undermine these security measures as described in the table below:

Lock Mechanism	Type	How it is broken
Signature (hand)	What you are	Signature forgery
Cheque book	What you have	Break-in / Stealing
ATM/Credit Card	What you have	Card cloners/stealing
ATM/Credit Card Pin	What you know	Skimmers/Camera/ Shoulder Surfing
Internet Access (Username + Password)	What you are + What you know	Phishing links that look like the bank website
Internet Access (Phone number)	What you have	SIM Swap
Internet Access (OTP)	What you know	Social engineering, Device Takeover (via phishing links)
Internet Card Transaction	What you have	Data leaks, Phishing
Micro ATM (Aadhaar Payment)	What you are	Fingerprint cloning
UPI (mPIN)	What you know	Account takeover via OTP to reset mPIN
Internet Access (Soft or Hard Token device)	What you have + What you know	Break-in / Stealing

Table 2. Approaches to override protective measures

Another aspect that is often poorly understood is the cost of implementing the lock-break mechanism. The table below outlines the cost for the scamsters against approaches to override protective measures.

Lock Mechanism	Type	How it is broken
Signature forgery	High to Very High	Signatures must closely match that with the records maintained by the financial institution. Further this is not scalable as it assumes cheques are obtained through break-ins and were not reported/stopped.
Card Cloners	High to Very High	Cloning cards require malware deployment and cloning equipment [9] [10]
Skimmers	Medium to High	Skimmers need to be deployed correctly to capture PINs and read card data via custom boards and hardware.
Phishing	Very low	Creating a phishing site that looks like an existing bank website/Payment Gateway/-Legal business is too easy. Coupled with SMS/Email messages, this attack can be executed with relative ease.
SIM Swap	Medium to High	While a Physical SIM Swap requires lax or active participation of telecom provider's staff[11] , takeover via eSIM conversion is possible with social engineering attacks.
OTP Phishing	Very low	Phishing to make the victim click a link to install VNC or Team viewer (OR) Social engineering to make them reveal an OTP is scalable as per attempt cost is very low.
Fingerprint cloning	Very low	It only costs about Rs.10/- to clone a fingerprint and the process is quite scalable because of widespread use of Aadhaar authentication for a variety of services. [12]

[9]Visa, New Malware Samples Identified In PoS Compromise. [Online] July 2020. http://click.broadcasts.visa.com/xfm/?40254/0/e72e19883ebb78a475570ab6dd5275ad/lonew

[10]With the widespread use of chip cards the ability to clone cards will reduce significantly.

[11]Companies have "vicarious liability" so they will have to be held responsible for the lapses. But this could also be done by "authorized" agents and retailers, making it difficult for the Telecoms to prevent it.

3. METHODOLOGY AND FINDINGS

Given this background, it is possible to formulate a few hypotheses on what analyzing a payment fraud dataset would reveal.

- H1: Scamsters will always attempt to use the break-in approach that has the least cost of execution and highest possible success rate.
- H2: The average value of the money taken out, through the break-in approach that has the least cost, will be equal or higher than the average value of the value money taken out, through approaches that have higher cost. (e.g., Cheque fraud will be high value-low volume and cyber fraud will be low value-high volume)
- H3: Investigators will generally struggle to resolve payment fraud cases that use low-cost break-in approaches, as it will overwhelm the investigation apparatus due to high volume.

While H1 and H2 above require quantitative data on modus operandi and money lost for validation, H3 can be validated using a qualitative approach by interviewing the investigators.

As there are no public datasets that were available which shows modus operandi and amount lost, the researchers teamed up with the Gurugram Cyber Police Station, which oversees all cyber cases in Southern Haryana. With the help of then DCP (East) Mr. Chander Mohan, IPS and ACP Karan Goel (DLF and Cyber), 1,228 First Information Reports (FIR) registered between August 2019 and September 2020 were manually analyzed by investigating officers, who categorized them as per the data schema in the table below[13] :

Field Name	Field Description
Date	Date of registering the FIR
Victim's Bank	Name of the Bank in which the victim held their account ('Unknown' if unclear)
Wallet	Wallet Provider Name (Left blank if unclear or unknown)
Notice to	List of entities to which CrPc Section 91 notices were sent asking for more information
Credit Card	Is there a credit card component involved?
Stolen Via	Description of the Modus Operandi
Refund Status	Was the amount given back to the Victims?
Information with Accused	Was the Victim's Personal information known to the Accused?
Amount	Money extracted (in INR)

[12]VLeena, Dhankar. Five held for cyber theft of 1 crore from 45 Palwal residents. [Online] July 2021. https://www.hindustantimes.com/cities/gurugram-news/five-held-for-cyber-theft-of-1-crore-from-45-palwal-residents-101623086919694.html
[13]Researchers were not provided with other sensitive PII by the investigators.

The following normalization process was then carried out by the researchers to clean up the dataset:

- Victims' Bank names were standardized and compared against the Reserve Bank of India's master list of scheduled commercial and co-operative banks (e.g., SBI, State Bank were normalized to State Bank of India).
- Wallet names were normalized.
- Entity names to which notices were sent was normalized.
- Amount value in other currencies were converted to Indian rupees at an average exchange rate during the period.

For validating H3, the researchers interviewed all the 22 investigating officers attached to the police station, with every interview session lasting an average of 30 minutes. All the interviews were recorded, transcribed, translated, and then summarized.

3.1. INVESTIGATOR INTERVIEWS – A QUALITATIVE ASSESSMENT

This part of the study uses an ethnographic method to understand the hurdles that come in the way of successful investigation and prosecution of financial cyber-crimes and is based on detailed interviews of cyber-crime police investigators posted at the Cyber Crime Police Station, Gurugram, Haryana over a period of three months. It also uses several case studies that are under investigation or under trial.

The interviews and cases reveal a complex set of reasons that lead to a poor conversion of complaints into First Information Reports (FIRs). This prevents investigation of most complaints, allowing scamsters to continue targeting individuals. However, the inability of investigators to successfully see through an investigation is due to several factors such as regulatory issues, lack of technology, limited access to data, inadequate training and poor processes followed by banks, payments' banks, payment gateways, merchants, digital wallets, and aggregators.

Investigators struggle with private corporations who either refuse to share data or do not have the legal cover for sharing sensitive personal data that could prove critical in investigations. These factors have been examined in detail in this section.

3.1.1. NPCI & DATA SHARING

The decision by NPCI (National Payment Corporation of India) not to share data with LEAs (Law Enforcement Agencies) was seen as a big blow by all the interviewed personnel. The inability of banks, payment gateways and merchants to share data on transactions is perhaps the biggest hurdle for LEAs in tracking cyber-crimes. Until July 2020, NPCI had a mechanism to share data with LEAs. However, NPCI which can track financial transactions through its switches, decided to not share this data anymore. This came as a big blow for those investigating cyber-crimes.

The payment merchants or victims' banks are frequently unaware of who the next beneficiaries are. Since that information is usually held by NPCI, this creates a major hurdle for investigators. By the time information arrives of a payment processed by an offender, the money has passed through several digital wallets and accounts before the money is converted into cash. As a result, the investigators seeking to track multiple transactions are always several steps behind the offenders who make the money pass through multiple wallets and accounts before retrieving the cash.

3.1.2. MULTIPLICITY OF AUTHORITIES

Most investigators dealing with cyber-crimes must deal with a plethora of authorities and regulators to access key data that is needed to successfully investigate and prosecute. On an average, the investigators must deal with six to eight different entities just to gather the basic facts needed to access data.

Data related to financial transactions are retained in part or whole by NPCI, the banks, payment banks, payment gateways, merchants, and aggregators. The guidelines and mandates issued by the RBI from time-to-time lead to changes in what data can be shared, by whom, to what extent and under what circumstances.[14]

Similarly, telecom related data is held by the telecom companies and are subject to rules and regulations issued by the Department of Telecom (DoT) and the Telecom Regulatory Authority of India (TRAI). The coming of a Data Protection Act and Authority will add another layer of regulatory restrictions on the sharing of data needed by police investigators to investigate and prosecute cyber-crimes.

A case in point is the struggle investigators face to get a mobile number being used by a scamster to carry out a series of frauds. While the police issue notices to the concerned telecoms, they are often advised to come through the Department of Telecom to get the numbers blocked. While this may protect a mobile phone user from getting a number blocked suddenly, this leaves the investigators in a difficult situation where the same numbers are used for repeated cyber-crimes while telecoms dither on blocking the numbers.

3.1.3. SECTION 78 MANDATES THAT ONLY POLICE INSPECTOR AND ABOVE RANKS CAN INVESTIGATE CASES UNDER SECTION 66

The Indian Penal Code (IPC) sections usually used for investigating crimes are sections 420 (Cheating), 120-B (Criminal conspiracy), 406, 467 and 468. Following the investigation, they add section 66 of the IT Act. The delay in adding Section 66 of the IT Act is deliberate. This section requires that cyber-crimes must be investigated by an officer of or above the rank of a Police Inspector. This puts an inordinate pressure on most police forces in the States since Police Inspectors are usually charged with manning police stations.

Police Inspectors are the cutting edge of any police force and have a plethora of duties to perform that ranges from overseeing investigations to carrying out law and order duties, which range from regular patrolling, managing crowds and manning stationary posts for crime prevention. Cybercrime investigation, hence, takes a back seat as there is little to no time left after carrying out these duties for officers of the rank of Police Inspectors.

The problem is also compounded by the fact that officers are only 15% of the total force as compared to the constabulary of any state police force[15] . Saddled with many administrative duties, senior officers have even less time to carry out investigations on cybercrime, which have low yields (successful conviction).

In Haryana, the current crop of officers at the level of Inspectors were recruited between the years 1994-1996. The crime scenario in a large part of their careers had a low exposure to internet bandwidths with low bandwidths and internet-related technologies. This has added to a major gap for Inspectors to investigate financial cyber-crimes, while the younger constabulary that has witnessed higher internet bandwidths and more exposure to technology don't meet the criteria laid down in the IT Act.

[14]The IOs have full authority to call for any record, CrPc overrides any regulation by RBI in this regard. For effective investigation
a. Information of POCs should be available with the LEAs through a standard process.
b. There should not be a single nodal officer.
c. Banks should publish the turnaround time.

[13]Total number of police officers is 15% of the overall police strength in India according to BPR&D. The recommendation by NASSCOM has been to amend the IT Act and allow Sub Inspectors to also carry out investigations as the Investigating Officer (IO).

Even adapting to a mobile phone and app-enabled environment has led to a rapid rise in cyber-crimes, and many senior officers at this level are still struggling to even catch up with current measures such as the (Crime and Criminal Tracking Network and Systems) CCTNS project[16].

3.1.4 . COMPOUNDABLE OFFENCES

A major hurdle to investigating cyber-crimes is the fact that the cases are compoundable. Offences that are listed under section 320[17] of the Indian Criminal Procedure Code can be compounded[18] , which means, the cases can be settled with the agreement of the victim (or accuser) of the offence. Cyber-crime investigators find the compounding of offences as a hurdle since it allows offenders to get away by returning the amount to the victim.

Investigators point out that most offenders of cyber-crimes dupe multiple victims. However, investigations are based on complaints received. The investigators build their cases using the evidence gathered by them. However, once the case goes to trial, the victim chooses the option to settle the case as soon as the offender agrees to return the money. The offender is then let off by the court, thus allowing them to continue duping others since going to jail is no longer a deterrent.

For investigators, this also leads to a major loss of motivation to see meticulously built cases coming apart as soon as the offence is compounded. Once the offender is let off, he/she is free to continue targeting fresh victims. Hence the organized nature of financial crimes requires a separate strong legal provision.

3.1.5. THE IMPACT OF ARNESH KUMAR VS STATE OF BIHAR JUDGEMENT

The Arnesh Kumar vs State of Bihar[19] , a judgement of the Supreme Court in 2014, issued detailed directions pertaining to the power of the police to arrest individuals. The facts dealt with the excessive and frequent use of Section 498A of the IPC read along with the Dowry Prohibition Act, 1961. Procedurally, the judgement shed light on Sections 41, 41-1 and 57 of the CrPC (i.e., the power of the police to arrest without warrant) and issued directions that would ensure "proper exercise of balance between individual liberty and societal order while exercising the power of arrest."

The directives passed in this case were made applicable to all cases where offences carry terms for imprisonment that are less than seven years or up to seven years (with or without fine). In this case, the Court was of the view that arrests must not be made 'unnecessarily' and that officers should refrain from making arrests until they are reasonably satisfied after investigation into the legitimacy of the allegations. The Court went one step further and held that officers will, in addition to departmental action, also be charged with contempt of court. It also placed requirements on the Magistrates to not authorize detention in a casual and mechanical manner, which if flouted would open them up for departmental action by the concerned High Court.

The judgement, thereby, places an obligation on law enforcement (police and the magistrates) to adhere to a clear set of safeguards while arresting an individual without a warrant in contravention of which they will be eligible for action. The impact it has on investigation is the need for the police to investigate an allegation (complaint) thoroughly to a satisfactory level before effecting arrest and not arrest an individual solely based on a complaint. Prohibition of casual arrests after this judgement is also covered under CrPc section 41A. Arrests can still be made with proper justification and the processes should be set in such a way that justifications are recorded[20].

[16]See NCRB CCTNS https://ncrb.gov.in/en/crime-and-criminal-tracking-network-systems-cctns
[17]Government of India. Section 320 in The Code of Criminal Procedure, 1973. India Kanoon. [Online] 1973. https://indiankanoon.org/doc/91933/
[18]Ayushi Tripathi, Compounding of Offences, 2019, [Online], https://lawtimesjournal.in/compounding-of-offences/
[19]Arnesh Kumar v. State of Bihar, (2014) 8 SCC 273, [Online], https://indiankanoon.org/doc/2982624/
[20]The organized nature of financial cybercrimes needs to be recognized and State laws an either amend or create new laws to deal with them. Maharashtra has the MCOCA (Maharashtra Control of Organized Crime Act) that helps LEAs to tackle such cases. However, records also show a high propensity to misuse laws such as MCOCA and due care should be taken to prevent misuse.

3.1.6. OTP LOOPHOLES

The single biggest loophole in all transactions cited by nearly all investigators is the two-factor authentication process via an OTP which is generated and delivered through an SMS. This has led to multiple kinds of frauds that are perpetrated by online scamsters and there had been instances of OTPs being passed on by bank employees. For most victims, the OTP is considered an authentic transaction. However, scamsters set up the intended targets by informing them that they will receive an OTP. They call up the victim and ask them to share the OTP as soon as it is delivered.

Even though many OTP messages specifically state that it is not to be shared with anyone, this is largely ignored by most customers. This results in not only aiding the scamster in getting access to payments, but it also enables them to gain control of the wallet or bank account on several occasions. This ensures that the scamster is now able to siphon off larger amounts from their victims as they gain administrative control over their wallets and accounts.

Many of the financial cyber-crimes are conducted by scamsters by tricking the intended victim into downloading a screen-sharing software. This makes OTPs received via SMS especially vulnerable. Many investigators believe that OTP via SMS is a flawed method. Instead, they suggest that OTPs generated over automated calls (Apple, Google and Twitter offer OTPs over call) can reduce this to a certain extent. Some banks have started a three-factor authentication where separate OTPs are sent to the registered mobile phone as well as registered email. However, since there is a vast digital divide with many people without access to the internet, this level of three-factor authentication will have low adaptability.

Investigators who were interviewed for this study also point out that profiling of the intended victims is a key part of the social engineering process that is used to carry out most cyber-crimes. This aspect needs to be factored in while designing a two-factor security process that is dependent on OTP as the primary second step of the authentication process.

3.1.7. THE FAILURE OF KYC (KNOW YOUR CUSTOMER) PROCESS

Interviews with financial cyber-crime investigators and data on complaints reveal a series of major issues with the KYC (Know Your Customer) processes adapted by multiple stakeholders in the digital payments space.

A key aspect of ensuring security is the KYC mandate given by RBI for all financial transactions. The KYC is also applicable for those applying for new mobile phone connections. Both are integral to the investigation of cyber-crimes.

No KYC Oversight: Investigators pointed out that the accounts that receive the money fraudulently often have poor KYC or incorrect details. This proves to be a major hindrance to successful investigations.

One investigator pointed out a specific case involving a virtual bank[21] (or a Payments Bank Account), where KYC provided by the fraudster used the branch address of the same bank. This slipped through the system and when investigators sought details from the bank about the owner of the account, they found that the bank's branch address was sent as a residential address.

Fraudulent Data: A similar problem has been witnessed when it comes to KYC of mobile phone users. Most cyber frauds committed so far witnessed the rampant use of mobile phones by fraudsters posing as a bank's customer service center. When these mobile numbers are supplied by the victim to the police, their KYC details are either fraudulent or incomplete. Most of these numbers are generated in areas such as Jamtara or Deogarh in the state of Jharkhand, and often lead to incomplete investigations.

[14]State Bank of India, Virtual Bank Account, 2020, [Online], https://onlinesbi.com/personal/virtual_account.html

Multiple Stakeholder, Multiple KYCs: The digital payments ecosystem has multiple stakeholders who seek KYCs. There are telecoms that need KYCs while issuing SIM cards, as do banks and digital wallets. However, there are several problems between these stakeholders:

- There is no standardization of the KYC data.
- There is no harmonization of KYC – a person using a mobile number signing up for a digital wallet will feed in different details for the mobile service KYC and the digital wallet KYC.
- Long chain of KYCs – For instance, a person using an identity proof issued in Tamil Nadu, purchases a SIM card in Jharkhand, moves to Rajasthan and uses it to target a victim in Maharashtra. This leads to multiple jurisdictions and conflicting KYCs for LEA investigators.

Inadequate cooperation between State Police: The fact that investigators must travel to different states for investigating cyber-crimes is further complicated by the fact that incomplete or inaccurate KYC forms of the fraudsters make it virtually impossible to track them down. The investigators also point out that cooperation with the local police of the states where the scamsters reside become difficult due to the poor implementation of KYC norms.

Tracking KYCs: Another problem with some payment banks, discovered by investigators, is the practice of shifting the KYC to fresh accounts. While this was a problem earlier, it has been addressed partly. This ensured that inadequate or faulty KYCs managed are passed on to new accounts, creating more complex problems for investigators. Scamsters are known to use multiple accounts to transfer funds quickly to stay ahead of the investigators. By the time investigators manage to track down multiple transactions, the money is withdrawn and disappears.

The local police also depend on KYC and even attempts to use the Base Tower Location (BTS) of the mobile phone numbers in use by the scamsters prove inadequate to track them down. Many investigators feel that the use of section 102 of the CrPc could be used to either block the numbers or seize devices used by the scamsters as part of the evidence-gathering process if the KYC norms are enforced strictly.

3.1.8. SIM SWAP SCAMS

For years security teams of banks have been warning customers[22] of losing access to their bank accounts through a SIM swap. A SIM swap is the process where a mobile connection holder gets back to their telecom service provider and seeks a new SIM for the same number when it is damaged, lost or needs an upgrade.

However, scamsters now pose as the owners of those mobile phone numbers and engineer a replacement of a SIM, using weaknesses in the two-factor authentication process[23] to take control of the phone number. This immediately opens a range of possibilities for the scamster, who can now find a way around the two-factor authentication process and gain full control of bank accounts or mobile banking applications. This also involves a degree of social engineering where scamsters gather enough data on their intended targets through social media and other means.

In a case involving a private sector bank in India, the cyber-crime unit of Gurugram police found that the scamsters were using a hit-and-trial method of discovering the bank's customers through their mobile phone numbers. This private bank allows customers to use their registered mobile phone numbers to log into the bank account.

[22]9. HDFC Bank. SIM Swap. HDFC Bank. [Online] 2018. https://www.hdfcbank.com/personal/useful-links/security/beware-of-fraud/sim-swap
[23]Norton Security. SIM Swap Fraud Explained. Norton. [Online] 2019. https://us.norton.com/internetsecurity-mobile-sim-swap-fraud.html

Scamsters who bought phone numbers in bulk from the grey market would keep attempting to use these numbers on the Bank's login page until a number was recognized by the site as a registered customer. They would then use the "forget password" function to generate a new PIN or password. This also involved a social engineering method to convince the customer that they were sharing the OTPs with the Bank's legitimate customer service center. Once they had the OTP, they would use it to gain access to the mobile or internet bank accounts and go on to make illegal transfers.

A related issue to SIM swaps is the availability of e-SIMS provided by some of the mobile phone manufacturers and telecom operators. Since the e-SIMS are embedded in the device, it becomes easier for scamsters to do a SIM swap by convincing the Telecom carrier and the unsuspecting customer that the SIM needs to be replaced. While some telecoms have tried to address this, investigators feel that more can be done to prevent SIM swaps using the e-SIM facility.

COMPLEXITIES OF FINANCIAL CYBERCRIMES: AN ILLUSTRATION

First Information Report (FIR) No: 0227 of 2020,
Police Station: Gurugram Sadar,
Date of Registration: 16 March 2020
Sections: 66 and 66D of Information Technology (IT) Act (Amended) 2008, 34, 419, 420, 467, 468, 471 of the Indian Penal Code (IPC), 1860
Gurugram Police, Haryana

A few days before the Government of India announced a nation-wide lockdown to manage the Covid-19 pandemic, Gurugram Police chanced upon a major financial cybercrime that is unique in many ways. This case also highlights the many challenges that LEAs face while investigating such cases as well as the sophistication and complexities that present-day scamsters use to defraud their victims.

Accused Arrest: According to the FIR, officers of the Gurugram Sadar police station received a tip off from a confidential informant that a few alleged criminals were travelling in a car after defrauding customers of their banking, credit/debit card and ATM details. Based on this preliminary information the police set up a roadblock and intercepted the car with four occupants.

The FIR records that the police recovered 66 fake SIM cards (29 Idea, 26 Vodaphone, 11 Airtel) with 42 blank credit/debit cards with magnetic strips, a card reader, 117 fake ATM cards and a laptop.

Card and Bank Data Theft: Investigations revealed that the four were involved in a variety of frauds that involved stealing user data from credit and debit cards, banks, e-wallets, ATMs, and other digital payment systems. The four were also involved in transferring the stolen money using a maze of bank accounts and digital wallets spread across multiple states.

Intercepting One Time Passwords (OTP): One of the accused was employed with a company that had been selected by a prominent private bank to generate OTPs for all the banking transactions using debit and credit cards issued by the bank. This employee would use his access to the generated OTPs to help the co-accused contact the bank's customers posing as part of the customer care service. The access to the OTPs and the card details of the users helped the accused to allegedly defraud many customers running into millions of rupees.

Multiple Phones, Bank Accounts and Digital Wallets: The police recorded that the accused had managed to set up multiple SIM cards to defraud victims and multiple accounts across banks digital wallets spread across several state like Delhi, Haryana, West Bengal and Karnataka to transfer stolen amounts to prevent tracking by LEAs.

3.1.9. PROBLEMS OF THE DYNAMIC IP

A common problem that many investigators now point to with cyber-crimes and frauds is the use of dynamic IPs by telecom companies. Depending on the usage, telecom companies allocate dynamic IPs to their users to ensure the optimal use of their allotted spectrum and bandwidth.

Static IP, which remains constant, is easier to track as far as evidence collection is concerned. Since the IP address remains the same, it makes it far easier for the LEAs to track the origin of the attack/ establish a chain of events. However, with dynamic IP this is not the case. Usually, dynamic IP addresses could be allotted for specified periods of time- days, months, etc. While trying to ascertain the source of cyber-crime, wherein there has been the use of the dynamic IP, investigators face major problems in using it to prosecute cases under the Indian Evidence Act by failing to meet the standards of electronic evidence.

Electronic evidence in India comprises broad categories of evidence in its digital form, data from digital devices or data relating to those digital devices. Since when the use of dynamic IP addresses is undertaken, IP addresses in use are actually *"borrowed from a pool of IP addresses, shared over various computers"*[24] , thereby making it difficult for investigators to narrow upon the user's identity that has committed the crime.

Additionally, requirements for analysis and certification under Section 65B of the Indian Evidence Act are also made hard in this regard when it is difficult to identify the user that has committed the crime. For any proof to be used as evidence relating to electronic record, its admissibility in Court is decided based on these conditions/certifications as prescribed in Section 65B of the Indian Evidence Act.

These conditions include forensic analysis methods and safeguards that are necessary for establishing chain of custody. Authenticity of the output in question and allowing for the evidence to be admitted in the absence of production of the "computer holding the original evidence" are some other conditions.

Problems in prosecution arise since Courts in India do not allow for admissibility of electronic evidence that do not meet these standards laid down under Section 65B of the Indian Evidence Act. Additionally, the non-reliability of IP address data rarely allows for prosecution solely based on IP address data, especially when dynamic IP processes are involved[25]. Better access to IP logs from telecom companies and KYC data, will thus ensure speedy investigation and conviction[26].

3.1.10. LACK OF CYBER-CRIME INVESTIGATION TRAINING

The process of posting to cyber-crimes does not factor in any specialized training for most police personnel. As a result, most of the training and specialized investigation skills are learnt on the job. This is a major lacuna that needs to be addressed by the bulk of the state police forces. While Haryana set up two specialized cyber-crime police stations, even the best police investigators feel the need for some specialized training course that addresses the kind of challenges that they face.

Often training and workshops are organized by using private resources of companies that regularly deal with cyber-crimes or frauds. However, from understanding the relevance of IPs, to gathering and examining electronic or online evidence so that they hold up in a court during trial are key issues that demand more focused training.

[24]Ministry of Home Affairs. CYBERCRIME INVESTIGATION HANDBOOK FOR POLICE OFFICERS. NIC. [Online] 2018. https://ssb.nic.in/WriteReadData/LINKS/5%20days36c9f227-7ceb-4b60-bada-f52beeb7e196.pdf
[25]Mudagal, KS. State of Karnataka vs Avinash R Kashyap. India Kanoon. [Online] 2018. https://indiankanoon.org/doc/52138604/
[26]Azad, Analyzing the National Security Implication of Weakening Encryption, 2022, Online, https://thedialogue.co/wp-content/uploads/2022/01/Report-_-National-Security-Encryption-_-The-Dialogue-DeepStrat-_-Jan-12-2022.pdf (Page 16, Metadata and Investigations)

Investigators also point out the peculiarity in investigating and prosecuting cyber-crimes, which are unlike other cases. A case in point is the policies of certain gateways for refunding money to customers who complain that the payment was done fraudulently. On many occasions, scamsters use multiple accounts and means to target their victims. Investigators chasing a fraudulent payment suddenly face a challenge when the funds in a particular complaint under investigation is refunded to the victim. While this is beneficial to the customer and leads to a quick resolution of their grievances, it brings a stop to an ongoing investigation and removes the subsequent possibility of prosecution of the cyber fraud. The process of refunding by payment gateways also alerts the scamster that the case is being investigated. This early warning to the scamsters also ends up leading to the closure of several complaints and cases.

The lack of specialized and focused training is further compounded by the lack of adequate resources. Most investigators struggle for laptops, desktops, internet bandwidth and power back up for carrying out their investigations. While most crimes can still do with analogue systems and paper records, cyber-crimes need basic tools and resources to carry out such investigations. The lack of adequate budgetary support also leads to chronic shortage of more specialized equipment that can be used for successful cyber-crime investigations.

The successful investigation and prosecution of a case is the most potent tool to deter scamsters. However, once the money is refunded, the case is closed and the scamster is now free to try their luck targeting other victims using different means. This leaves investigators to constantly try and catch a scamster and bring the case to a successful prosecution with little success.

3.2. FIR (FIRST INFORMATION REPORT) DATA

Police FIR is one of the most reliable indicators that a financial fraud has indeed been committed. While direct complaints to the financial institutions is an indicator, that dataset also contains service-related complaints and hence is prone to over-estimation without a costly cleaning exercise. However, filing a Police FIR requires time commitment and a conviction by the victim that they have been defrauded and does not require data pruning to ascertain if it is just a service delivery issue or a crime.

The FIR data however has a few caveats:

- The Cyber Crime division in Gurgaon only caters to one half of the state of Haryana and, hence, it is not possible to claim that this data is representative of all of India and extrapolate the results. However, it is representative of the State of Haryana for the time chosen.

- Police FIRs are not digital documents but are mostly on paper. Hence for data analysis, these had to be converted into a machine analyzable form, by reading through all the FIRs, the action taken and categorizing the modus operandi, manually. In-advertent errors might have crept in, even though double checks were carried out by case officers, while categorizing modus operandi.

3.2.1. MODUS OPERANDI

The FIR data after normalization yields a set of modus operandi which needs to be explained in depth to understand both the operational, tactical, and strategic aspects of the crime operation, that makes the scamsters successful in the field. The table below provides the list of modus operandi and a short description, with longer explanation elsewhere.

Modus Operandi	Short Description
ATM WITHDRAWAL	Unauthorized ATM withdrawal without any contact with the victim.
BANK EMPLOYEE	Bank employee precipitated the fraud
CARD SWIPE	The Debit or Credit card was physically swiped to carry out an unauthorized transaction.
INSECURE WALLET	Wallet has been picked and the Card was used via NFC near-field communication).
KYC LAPSED	The victim was told that their KYC had lapsed and was then led down a path that got them defrauded.
OTP SHARED BY VICTIM	The victim was told a convincing story that led them to share their OTP.
PAY VIA LINK	The victim was sent a payment link, clicking on which money was deducted from their account.
PROXIMA FRAUD	A popular method of fraud associated with digital wallet platforms/online payment system
QR CODE	The victim was shown the wrong QR Code that led them to pay.
SHOPPING SITE	The victim was sent a shopping site link for payment.
TEAM VIEWER APP	The victim was sent a link that installed the TeamViewer App on their phone, which was then used to control their device remotely.
UNKNOWN	Cyber Crime was not able to understand the modus operandi used.
VICTIM MONEY TRANSFERRED	The money was transferred by the victim to the fraudsters' bank account after a convincing story.

3.2.1.1. ATM WITHDRAWAL

A fraudulent ATM withdrawal always require two distinct sets of information:

- The Financial Instrument (Credit or Debit Card)
- The ATM PIN
- CVV

There are two ways to obtain the financial instrument in question – physical stealing or via card cloning. A Credit/Debit card always has some static information such as:

1. The 16 Digit Card number
2. Issue Date
3. Expiry Date

This information was put in the magnetic stripe in plain text format but over the years fraudsters learnt how to read them via custom devices and then replicate them to create cloned cards. This led to the invention of CHIP and PIN cards, where a computer chip is embedded in every card and generates random codes to the bank network for every transaction. Further to authenticate the transaction, the user must input a PIN (Personal Identity Number) in the device, for a successful transaction.

The RBI mandated all banks to use CHIP and PIN cards from January 01, 2020, onwards under the assumption that they would reduce fraud conducted via card cloning, if not eliminate it.

Even after cloning the card (magnetic strip cards), the fraudsters still need to obtain the PIN. Three common techniques are used to obtain the PIN:

- Deploying Trojans/Malware in the POS (Point of Sale) machines.
- Obtaining it from victims via phishing techniques.
- Obtaining it as part of card skimming itself.
- Pinhole cameras on ATM machines.

3.2.1.2. BANK EMPLOYEE

Insiders and particularly Bank employees, can always deploy multiple methods to defraud bank customers. For instance, they may simply leak customer information including Debit/Credit card details to others or may change the email IDs/Mobile numbers to which OTP (One Time Password) is sent or they may use a returned Debit/Credit card which could not be delivered to the customers.

3.2.1.3. CARD SWIPE

Card swipes are credit/debit card transactions carried out by fraudsters after cloning the card and obtaining the PIN as described in section "ATM Withdrawal". The key difference lies in the usage, where instead of using it to withdraw cash from an ATM, it is used to transact by swiping it on POS terminals.

3.2.1.4 . KYC LAPSED

KYC Lapsed is a modus operandi that is a unique Indian phenomenon and is a side effect of the regulatory and technological changes that happened in the payment landscape. The timeline of these events is summarized as below:

- Unlike other western countries, which had credit and debit cards as a first-choice payment instrument and which continued that path and then went to mobile phone payments, for most Indians, their first brush with digital payments was their mobile phone.

- This culminated in the rise of Digital Wallets – Apps to which money can be loaded from a bank account, credit, or debit card, which can then be spent on merchant establishments that accept these and for personal individual payments.

- Personal individual payments (referred to as P2P) were once again a uniquely Indian phenomena since there existed two types of economy – the formal economy where businesses are registered and the informal economy where the entrepreneur was not registered and hence accepted payments only in cash.

- The adoption of mobile phones meant that suddenly they could carry out their businesses with just a mobile phone, if they can accept payments from digital wallets.

- The demonetization event of November 2016 accelerated this trend as 86% of the circulating cash was declared as invalid tender in one night, thus leading to the era of the digital wallets.

- At that point in time, KYC norms had not been formalized, but that changed on October 11, 2017, when the RBI notified the KYC norms for PPI (Pre-Paid Instruments) also known as digital wallets.

- This was not well received by the digital wallet providers since it meant that transactions on wallets which are not KYC compliant as per the norms notified were not allowed.

- The RBI, hence, issued multiple deadlines and finally chose February 2020 as the last date for digital wallets to become fully compliant with the notified norms.

As this played out over a span of four years, another parallel sequence of events happened – the continuous push to link customers' bank accounts with Aadhaar under the threat of freezing the account as per the rules notified under PMLA Act (Prevention of Money Laundering Activities). While this was eventually struck down by the Supreme Court, these two sets of events created a situation in which wallets and bank accounts could be deactivated in a moment's notice because of the ever-changing KYC norms.

The economic disruption that a deactivated wallet or bank account can cause is quite strenuous to handle by citizens, who are increasingly nudged towards digital transactions. As there were multiple news articles, media announcements and SMS alerts from both the financial institutions and the government about Aadhaar linking and KYC norms during this period, it created an environment where any notification about an account deactivation because of KYC expiry, created a panic reaction that forced compliance.

This environment was exploited by the fraudsters, who could call the victims as agents of the wallets or Banks and simply tell them that unless they share an OTP or click a link, their wallet or Bank account will be deactivated for non-compliance of KYC norms.

The FIR data reveals two distinct set of operational success:

- Sending a transaction OTP to the victim's phone number in the guise of a KYC verification, which is then used to hijack their bank accounts.

- Sending them a link, which when clicked, installs a Trojan that takes over their mobile device completely and puts it under the fraudsters control, which allows them to see their m-PINs (Personal Identity Numbers used to make transactions in their Bank/Wallet Mobile Apps).

3.2.1.5 OTP SHARED BY VICTIM

The OTPs became a norm because of a technological change – the relentless march of computing power which made password cracking trivial. While passwords are typically stored in encrypted form, not every encryption algorithm is the same. Some are easily cracked, others are harder.
The approach used to crack passwords is a mixture of brute force, pattern analysis and intelligent guessing. With the advent of GPUs (Graphics Processor Units) which not only are good for playing games but are also excellent for cracking passwords, just relying on passwords alone for online safety was simply not good enough in the era of cloud computing.

The other trend that accelerated was of AFA (Additional Factor Authentication) or 2FA (2nd Factor Authentication) which is that humans are notoriously poor in remembering random passwords and always chose the same passwords or a variant of them for multiple accounts. Hence, compromise of one set of logins created a cascading effect where the cracked passwords were used to login to another set of accounts (via a technique called Credential Stuffing).

The RBI recognized this problem as early as 2008, where it mandated 2FA for mobile transactions. While it worked in mitigating fraud to a large extent, interactions between two larger trends outside of its control has weakened its impact namely –

- The population's lack of digital literacy in distinguishing between "secrets" told to an app (or a website) for availing a service Vs. revealing these secrets to a human.

- The explosive increase in the use of OTP by everyone (including for availing gym memberships and entry into apartment complexes) for a variety of purposes that not only normalizes revealing OTP to strangers, but also mixes up Authentication, Authorization, Identification.

An example of how pervasive the lack of digital literacy is can be recognized by a story by the Economic Times[27] . It documents how even victims, who are well educated and work in the IT industry, shared Debit Card numbers and CVVs (Card Verification Values) and even forwarded garbage SMSs (which are Secrets) to phone numbers of strangers who posed as Bank officials.

The key issue here is that a large section of population cannot distinguish between:

1. Public Identifiers (Name, Phone Numbers)
2. Private Identifiers (Debit Card numbers) and
3. Secrets (OTPs, CVVs)

This is because they don't have a basic understanding of Privacy. This allows fraudsters to call them up and convince them to share their "secrets" which the victims believe as harmless Private Identifiers. All that is required are messages embedded within the phone calls that appeal to the emotions of the victims such as:

- Offering an upgrade of their Credit/Debit Cards (thus providing them a sense of belonging to a unique and exclusive club which pampers their self-importance).

- Providing them a free tour package, cashback reward (thus creating a FOMO (Fear of Missing Out) effect.

- Threatening account deactivation because of lack of KYC compliance (a fear inducing effect that works because of the ground reality of ever-changing compliance rules).

3.2.1.6. PAY VIA LINK

A typical payment transaction between two parties involves an information exchange of:

- The Destination Bank Code (IFSC Code)
- Destination Bank Account number
- Name of the Receiver
- Transaction Amount
- Authorization of the Sender for the transaction (Typically a signature on a cheque).

Now except the last part (Authorization), all the above information can be put out by the receiver of the money like a simple rate card. And then a unique link (URL) can be generated which when clicked by a payment app, can do the final part of authorizing the transaction by the sender.

However, since the URL is under the complete control of the receiver, they can always substitute the "Name of the Receiver" field to any other name. This is possible because the Pay via Links feature is typically provided by Payment Gateways, which allow Display Names to be changed, along with logos.

This allows a fraudster to generate a payment link on the name of a well-known entity, even though the destination bank account number would be the one that they control. As indicated in the previous sections, the destination bank account in which the money lands, may not even be in their name, but the one they control without the actual holder being aware of it.

[24]ET Bureau, New Form of OTP Theft on rise, 2019, [Online], https://economictimes.indiatimes.com/news/politics-and-nation/new-form-of-otp-theft-on-rise-many-techies-victims/articleshow/67521098.cms

There are quite a few variants of the Pay via Link modus operandi:

1. Forging the name of the Receiver
2. Switching the direction of Payment – A fraudster may say to the victim that clicking the link is required to receive money, while they end up paying.
3. Rapid withdrawals by sending multiple links of which some are small credits, but some are large debits.

3.2.1.7. PROXIMA FRAUD

This is a common fraud that happens because of a vulnerability that allows overseas payment gateways to process payments on a credit card without an OTP. All that is required is the Credit card details and the CVV, which have been leaked to the fraudsters.

3.2.1.8. QR CODE

This is a slight variant of the Pay via Link approach, but instead of links being sent, QR codes are sent to the victim.

3.2.1.9. SHOPPING SITE

This is a slight variant of the Pay via Link approach, but the links are that of a shopping site to pay for goods, instead of a money transfer.

3.2.1.10. TEAM VIEWER APP

The mobile phone is a general-purpose computing device optimized for personal usage. While in theory, apps installed in the device are isolated and can't interfere or read the data of other apps, reality is much more complex. There are always root apps which are installed as part of the operating system, that can neither be uninstalled nor have their permissions revoked.

However, apps that allow remote controlling such as TeamViewer or viewing the phone screen in their entirety, can enable capturing of secrets such as mPINs (Mobile Personal Identity Numbers) and other private information like Debit Card number, Expiry date etc.

Once secrets are captured, it is trivial to withdraw money from the compromised bank account, load it into a wallet and then spend it away on online portals, thus making recovery impossible.

3.3. WHAT THE DATA REVEALS

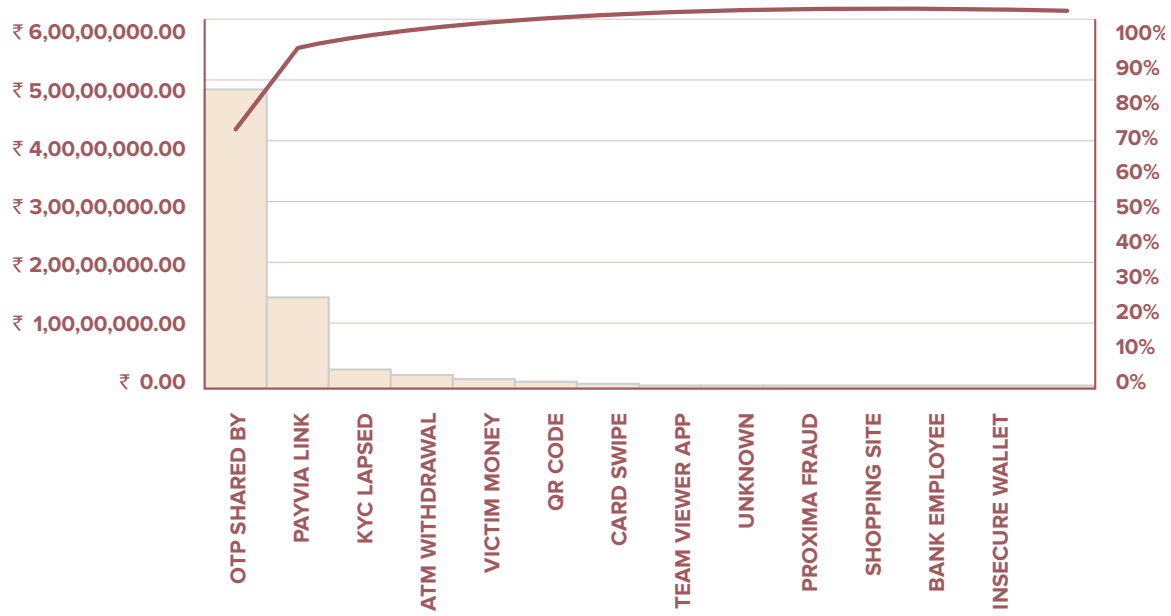
With a dataset sample size of 1,228 records across 11+ months with a total fraud of Rs. 6.89 crores, spread across 12 different modus operandi, the distribution looks as below:

Modus Operandi	Total Amount	Count of Cases
Otp Shared By Victim	₹ 4,76,58,432.58	821
Pay Via Link	₹ 1,43,39,975.07	220
Kyc Lapsed	₹ 24,94,142.00	67
Atm Withdrawal	₹ 15,53,656.00	48
Victim Money Transferred	₹ 8,53,300.00	3
Qr Code	₹ 6,96,446.00	33
Card Swipe	₹ 6,83,454.00	17

Team Viewer App	₹ 4,32,384.00	7
Unknown	₹ 1,12,231.00	7
Proxima Fraud	₹ 21,717.00	2
Shopping Site	₹ 21,000.00	1
Bank Employee	₹ 17,250.00	1
Insecure Wallet	₹ 10,000.00	1
Grand Total	₹ 6,88,93,987.65	1228

Table 3. Modus Operandi Distribution

A pareto plot of modus operandi vs. total amount, as shown below, indicates 80% of the fraud committed by amount can be attributed to a single modus operandi (OTP) and 95% of the fraud committed by amount are attributed to just three types of modus operandi.



This data proves the hypothesis H1 and H2, which was formulated earlier that:

- H1: Scamsters will always attempt to use the break-in approach that has the least cost of execution and highest possible success rate (OTP Stealing Attack)
- H2: The average value of the money taken out, through the break-in approach that has the least cost, will be equal or higher than the average value of the value money taken out, through approaches that have higher cost. (OTP Stealing Attack contributes to 75% of the Fraud value and 66% of the cases)

Further the third hypothesis, which theorizes that investigators will generally struggle to resolve payment fraud cases that use low-cost break-in approaches, as it will overwhelm the investigation apparatus, is also accurate as is evident from the qualitative interviews and the quantitative data.

3.3.1. PARETO EVERYWHERE

Another interesting aspect of this dataset is that, even within specific modus operandi, it is possible to find pareto distributions, where most of the fraud committed by amount is skewed towards high value. For instance, one can assign the following classification to the fraud value:

Categorization Rule	Category
Greater than 1 Lakh	XL (Extra Large)
Between 50,001 and 1,00,000	L (Large)
Between 25,001 and 50,000	M (Medium)
Between 5,001 and 25,000	S (Small)
From 1 to 5,000	VS (Very Small)

Table 3. Modus Operandi Distribution

Applying the categorization on the entire dataset:

Category	Amount	Cases	Case %	Amount %
XL	₹ 3,68,88,363.15	92	7.49%	53.54%
L	₹ 1,37,16,839.00	184	14.98%	19.91%
M	₹ 1,02,07,169.18	271	22.07%	14.82%
S	₹ 73,96,409.25	504	41.04%	10.74%
XS	₹ 6,85,207.07	177	14.41%	0.99%
		1228	100.00%	

Table 5. Pareto Distribution on Modus Operandi

The first two categories (XL and L) alone contribute to 73.45% of the fraud amount, even though by case count, it is only 22.48%. When the same method is applied for other approaches:

Category	Amount	Cases	Case %	Amount %
XL	₹ 2,55,77,667.15	65	7.92%	53.67%
L	₹ 94,93,136.00	127	15.47%	19.92%
M	₹ 73,84,010.18	197	24.00%	15.49%
S	₹ 47,35,665.25	316	38.49%	9.94%
XS	₹ 4,67,954.00	116	14.13%	0.98%

Table 6. Pareto Distribution on OTP Shared

Category	Amount	Cases	Case %	Amount %
XL	₹ 88,72,605.00	15	6.76%	61.87%
L	₹ 23,68,717.00	32	14.41%	16.52%
M	₹ 17,03,465.00	44	19.82%	11.88%
S	₹ 12,41,627.00	88	39.64%	8.66%
XS	₹ 1,53,561.07	41	18.47%	1.07%

Table 7. Pareto Distribution on Pay on Link

Category	Amount	Cases	Case %	Amount %
XL	₹ 7,84,765.00	5	7.46%	31.46%
L	₹ 8,16,549.00	11	14.41%	32.74%
M	₹ 3,89,438.00	10	14.93%	15.61%
S	₹ 4,90,538.00	36	53.73%	19.67%
XS	₹ 12,852.00	5	7.46%	0.52%

Table 8. Pareto Distribution on KYC Lapsed

Category	Amount	Cases	Case %	Amount %
XL	₹ 3,61,206.00	3	6.25%	23.25%
L	₹ 4,77,116.00	6	12.50%	30.71%
M	₹ 2,85,782.00	8	16.67%	18.39%
S	₹ 4,18,062.00	27	56.25%	26.91%
XS	₹ 11,490.00	4	8.33%	0.74%

Table 9 - Pareto Distribution on ATM Withdrawal

Each one of the modus operandi has a pareto distribution, which is quite unique and suggests a power law in play. To understand why this is important, consider how much the XL and L cases contribute across each modus operandi as shown below:

Modus Operandi	Cases %	Amount %
Overall	22.48%	73.45%
OTP Shared by Victim	23.39%	73.59%
Pay via Link	21.17%	78.39%
KYC Lapsed	23.88%	64.20%
ATM Withdrawal	18.75%	53.96%

Table 10 - Power law across Modus Operandi

Not only do the overall cases follow the 20-75 rule, but every sub-type of modus operandi also approximately follows the same pattern. In non-mathematical terms, this implies that frauds are scalable across every modus operandi and have outsized payoffs on a very small number of successful frauds, which increase the overall value of the frauds. So, law enforcement agencies only must solve a small number of high value frauds and bring down the networks that power them, which will eventually bring down the overall cases, over time.

3.3.2 WHY PARETO AND IMPLICATIONS

There are two ways to do retail cyber-crime, either through a network that produces linear payoffs or through a network that produces pareto pay offs. While the average payoffs in both modes may look similar, the back end that powers the networks will be quite different. To understand why crime networks tend towards Pareto, consider the infrastructure required to operate it:

- Fake identity or borrowed identity allows scamsters to procure mobile phone numbers, bank accounts and digital wallet accounts, along with email addresses.

- Through mobile phone numbers, they trick victims to reveal their OTP or forward messages that contain payment links or QR codes that can defraud them.
- Once defrauded, the money must be moved out very quickly to multiple accounts, to outpace the investigators, because every 'hit' is a potential jail sentence, if investigated.
- Given the randomness associated with picking victims, it implies that the payoff must be maximized for every 'hit' against the probability of a potential jail sentence.
- Played over time, this naturally makes all modus operandi follow the pareto distribution.

While the tendency for crimes to veer towards pareto increases public dissatisfaction and puts huge pressure on the law enforcement, there is a silver lining. The crime network will continue to reuse the same assets (Bank Accounts and Wallets in particular) and if a few cases are busted, it allows these resources to go offline as well. In one instance, busting a single operator revealed that they had access to 305 bank accounts, 10 Airtel payment bank accounts, 12 PhonePe wallets and 10 Ola Money wallets

The high reuse of infrastructure means, for every high value case solved, a lot of low value cases will be solved and could be attributed to the same operator. Hence law enforcement can shut down "a large number of crimes" by busting a small number of operators by using the Pareto principle in reverse.

If done correctly, it will increase the cost of getting busted for every attempt made and hence operators will over-correct by working to increase the payoffs further. Hence, if law enforcement is confronted with minimal resources for solving crimes, they should always focus on the high value cases.

4. WAY FORWARD

4.1. OTP ALONE IS NOT ENOUGH

There are several parties involved in an OTP transaction:

1. The recipient (who would receive the payment)
2. The initiator (who would start the transaction)
3. The financial institution in which the initiator held an account.
4. The telecom provider from which the initiator has obtained a mobile number.
5. The bulk SMS provider that the financial institution has signed up with for sending the OTP.
6. The template checker and message scrubber, which is responsible for checking if the OTP message is as per the TRAI DND regulations and delivering it to the initiator.

The involvement of several parties in the loop between the initiator and the financial institution creates fragility not just in the delivery of the OTP[28] , but also in terms of risk. For instance, Paytm sued telecom companies that they did not act against phishing companies and sued them for not doing enough[29]. Telecom companies argued back that it is not their problem, but it is Paytm that is responsible[30].

Given that investigation after a payment fraud is seriously hobbled as detailed in the previous sections, fraudsters don't have sufficient deterrence from operating freely and performing sophisticated social engineering attacks on the initiators, which succeed at scale. This is because they not only have access to their personally identifiable information (PII) through data leaks and other means, but also, they are able to reach them through a public identifier (Phone number).

While the intent of the RBI's regulations is to inform the account holders on transactions that happen on their accounts via SMS alerts and for transaction authorization, the same communication channel is now being used to defraud them, with neither the telecom companies, banks, payment gateways, wallet companies willing to address the problem as the investigators had clearly outlined. This affects account holders but also brings down the trust on digital transactions, thus bringing down the potential volume of the digital transactions.

While improving state capacity is one option, other technical options must also be thought through which reduces the chance of account holders falling prey to scamsters. For instance, account holders can be given multiple technical options to choose from rather than only having the option of using OTP delivered through mobile phones, such as App based OTPs (Google Authenticator[31] , AUTHY[32] , ZOHO 2FA, Bit warden etc.).

As they are based out of a common secret shared via QR Codes, which can be either delivered on the screen (via Internet banking credentials) or via a paper based QR (like how ATM PINs are delivered), account take-overs by compromising weaknesses in telecom providers' process can be mitigated.

Further in the interim, banks must limit enumeration attacks on mobile phone numbers through rate limit techniques, or perhaps disallow phone number-based login completely. This will disallow scamsters to check if a mobile number is indeed linked to a bank account.

[27]Deep, Aroon. TRAI-mandated spam filters catch OTP messages, hobbling SMS delivery. Medianama. [Online] March 9, 2021. https://www.medianama.com/2021/03/223-trai-spam-filters-otp
[28]Jalan, Trisha. Paytm alleges telcos did not act against phishing companies, approaches Delhi HC. Medianama. [Online] June 2, 2020. https://www.medianama.com/2020/06/223-paytm-phishing-telecom-delhi-high-court/.
[30]15. Deep, Aroon. In Paytm telecom fraud case, Jio invokes intermediary liability: Report. Medianama. [Online] June 22, 2020. https://www.medianama.com/2020/06/223-paytm-jio-ucc-fraud-intermediary-liability
[31]Google Authenticator, https://www.google.com/landing/2step/
[32]Authy 2FA, https://authy.com/

4.2. DATA SHARING REGULATIONS

Financial fraud investigation is only possible if all entities in the transaction pipeline agree to share data with one another when an incident occurs. For instance, when the fraud is committed by using payment wallets, a commonly observed pattern is that it is done through UPI registration of names in well-known e-commerce entities, but with a different domain name. Unwinding the chain is not possible without information sharing, but without an FIR, entities will not share any information to the victim.

Hence, it becomes imperative to evolve and define a data sharing protocol among financial entities for the purpose of fraud investigation by the regulator as uncertainty in this aspect ensures that fraudsters are never stopped on time.

4.3. DEDICATED PAYMENT FRAUD INVESTIGATION CELLS

Most online frauds are cross-state and in some cases even cross country (e.g., Chinese loan scam). This requires state units to cooperate across state boundaries and work with law enforcement in other countries via the MLAT (Mutual Legal Assistance Treaty) route. With transfers and lack of equipment, dedicated training investigators are not very effective as there is less institutional memory on the complexities associated with payment frauds.

Given the volume of frauds, perhaps the time has come to create dedicated payment fraud investigation cells at the national level.

5. RECOMMENDATIONS AND CONCLUSION

a) There is a need for a dedicated effort to collect empirical data on cyber payment frauds to assess the magnitude of the problem countrywide.

b) A regulator such as the Reserve Bank of India needs to standardize safety features and processes of all stakeholders in the digital payments' ecosystem for greater harmonization and safety of users. This will also aid LEAs in reducing their effort to carry out successful investigations of financial cyber-crimes.

c) A data sharing standard across all stakeholders to ensure timely access to law enforcement for investigation.

d) Organizations like the NPCI or the proposed NUE must have a mechanism for identifying and tracking transactions linked to financial cyber-crimes to ensure speedy tracking and resolution for LEAs.

e) Cyber-crimes are complex cases from an investigative point of view and therefore the provisions to make these cases compoundable should be reviewed.

f) The IT Act under section 78 mandates that only an Inspector or above rank of police can investigate cases registered under section 66 of the law. This needs to be reviewed to increase the pool of investigators available in the States.

g) Cyber-crimes need regular and specialized training capsules for LEAs from information security researchers and academics to stay

h) Cyber-crimes need regular and specialized training capsules for LEAs from information security researchers and academics to stay abreast of the latest techniques deployed to commit financial frauds or to even prevent it.

i) The KYC norms don't work for investigators and LEAs since multiple cases have been found with inadequate or fraudulent credentials. These need to be reviewed and strengthened.

j) Regular checks of sample KYCs to be carried out at regular intervals as an oversight mechanism with penalties on Telecom/Bank officials for irregular entries.

k) States where cyber-crimes originate should appoint a dedicated police officer to liaison with other States to enable investigation, arrests and prosecution and coordinate with the Union Ministry of Home Affairs, India Cyber Crime Coordination Centre (I4C) and Regional Cyber Crime Coordination Centre.

l) There can be an escrow arrangement by banks and digital payment companies to minimize losses to a customer due to financial cyber frauds.

m) There should be a look at TRAI's bulk messaging regulations to see how they can be used to prevent any interception of OTPs or messages aimed at defrauding users.

6. ACKNOWLEDGMENTS

The authors would like to acknowledge the help and generous cooperation extended by several institutions and individuals who spent time with the researchers to share data and insights. We would like to thank the Haryana Police, the Director General of Police, Haryana, the Commissioner of Police, Gurugram and all officers of the Gurugram Police Commissionerate. Some officials of Faridabad Police Commissionerate also extended their help and insights for this study. The officers and constabulary of Cyber Police Station, Gurugram, and, Assistant Commissioner of Police (DLF and Cyber), the Station House Officer, Cyber Police Station, Gurugram and the MHC, Cyber Police Station Gurugram and all the other officers and investigators who spent days helping us.

We would also like to thank cybersecurity teams of various card and digital payment companies, banks who generously shared their insights. Some officials dealing with financial cyber-crimes in the Union Ministry of Home Affairs also shared valuable insights and we thank them for their help. We also thank Ms. Neha Sarah Noushad who helped us track news reports on financial cyber-crimes. Finally, we would like to thank several information security researchers who spent time helping us with their insights and analysis of the data.

DEEPSTRAT
STRATEGY . POLICY . ACTION

The Dialogue™
INFORM ENGAGE IDEATE

A study on problems faced by LEAs in investigation and prosecution of financial cyber crimes in India by Saikat Datta, Chander Mohan (IPS), Anand Venkatanarayanan and Kazim Rizvi.

https://deepstrat.in https://thedialogue.co