IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 10, Issue 1 - V10I1-1192)
Available online at: https://www.ijariit.com

Role of technology in finding planned defaulters

Ananya Bhatnagar
pavini@yashishukla.com
Amity Pushp Vihar, New Delhi, Delhi

ABSTRACT

The paper focuses role of technology in finding planned defaulters. With the fast pace advent of financial technology, it is imperative that technology plays a key role in enhancing customer experience esp. around security and preventing default. The paper identifies the role of technology in identifying planned defaulters and how it can be adapted and used for preventing such mishaps from happening in future. A quantitative survey has been undertaken, which shows fast adoption of fin tech solutions by Merchants/small scale businesses. The survey also highlights the concern of risk associated with the fraud and how well the Merchants can adapt to tech solutions to prevent such incidents, thereby enabling technology to play a firm role in identifying planned defaulters. The paper summarizes current methods used on finding planned defaulters by fin tech companies and what should be done further in this area. The paper also lays out future scope of research work.

Keywords: *Technology, Debt, Planned Defaulters*

I. INTRODUCTION

Shubhangi runs a small kiosk from her humble abode but in order to meet the evergrowing demands of her family she also works as a house help, one of the houses were she worked was ours. We were happy to have such an honest, diligent and cheerful help. It was 5th of June, I clearly remember I was on a videocall with my granny as it was her birthday. Shubhangi entered the house , panicked and distraught clearly not her usual self. We abruptly ended our call and rushed to her. She was duped while making online transactions , all her savings puffed in air in the blink of an eye. All our efforts to console were in vain and we also felt its sting and pain. My parents helped her to report this to cybercrime branch. This was first for me and I felt stongly for her as I have been witnessing her struggles day and night.

Sushma runs a tiffin centre from her home. She also works as a part time cook in my friends house. Due to convenience involved with digital transactions and home delivery apps she switched to this mode. Once while paying by digital wallet , the vendor told that he hasn' t received the payment which she already made. He then asked her to click a link so that lost payment can be retraced. She did so and lost her money in savings accounts.

Experiencing these unforeseen and unfortunate incidents upclose I was filled with anger and shock. Was there any solution to their problems? Have people completely lost their humanity ? Such questions and many more like these kept hovering in my head endlessly. In my heart I knew that one day I am going to work towards something which can bring solace to such grieving hearts

I have always been intrigued by technology and finance . It was just a regular day for me , I was scrolling through social media , where there were many articles about fin-tech and its future scope . But one , that caught my eye was on a new gadget called 'Fraud Finder' . I was so intrigued by it that I decided to dig deeper in it . How could technology and fraud can be inter-linked? This was something that was mind-boggling for me . This was the first time I came across the term fin-tech . I then further read articles about Fraud Finder. It was designed to identify planned defaulters and prevent financial losses .

I was curious to know more. They used advanced algorithms and data analysis to uncover patterns, detect suspicious activities and also future prospects. This was something that opened my eyes to the world of technology and fraud. We live in a digital world and more and more people are getting accustomed to it as it is easier and convenient way for transactions. Unfortunately it also increases the risk of fraud . This also helps to prevent innocent hardworking people from falling in such traps, hence I decided to work on this topic and give my inputs on it.

It is common knowledge that there are two types of defaulters, those who do not pay because of cash flow problems ('Can't Pay'), and those who do not pay because of lack of willingness to pay ('Won't Pay').

A wilful defaulter can be:

- can be when a person/institution refuses to pay even when they can pay the said amount.
- Funds are not utilized for the specific purpose but have been diverted for other purposes.

Several techniques have been proposed by numerous researchers, we refer readers to excellent research (Liu, Fan et al., 2014) and surveys (Crook et al., 2007). Traditionally, banks are allowed to build their own credit scoring models to risk assess their customers and arrive at suitable scoring models to arrive at credit worthiness of loan applicants (classified as credit worthy or credit worthless). Dozens of techniques have been proposed by numerous researchers. Most of these approaches require a large sample that contains properly labelled customers based on their history over a long period. Such assignments are not always available, especially for long-term products, which limits the applicability of such methods in practice.

We refer to research work of (Liu Fan et al. 2014), regarding example of building scorecard for one of China largest commercial bank in year 2008. Samples were selected from existing accounts where the average term of loan was over 10 years. The paper refers to customers rarely default immediately after taking the loan. It will take some time before a sufficient number of defaults to train any meaningful model – in this case 24 months. The defaulting labels for customers were then determined according to their behaviour before 31st December 2008 rather than the loan lifetime. However, the non-default group included customers that may default after the this time. This work concludes that directly applying a classification-based method to this data set was inappropriate.

We also refer to work (Andreeva, Ansell, and Crook, 2007), who introduce a combination score method to capture the relationship between the customers' profitability and the time of default. The paper presents the first empirical investigation of the relationship between present value of net revenue from a revolving credit account and times to default and to second purchase. The paper includes the survival probability of default and the survival probability of second purchase (a survival combination model) rather than merely a static probability of default.

We retain desirable properties from the above analysis and do more research in Indian context. We complement it by use of technology in "real-time" finding planned defaulters. With the help of technological model where we use machine learning, data analytics and artificial intelligence(AI) to analyze data, transaction records, identify patterns and help in finding potential defaulters. Machine learning can detect early wavering signs of default(from historical data or current data given as input patterns), allowing institutions to intervene.

Before we go in how technology can help detect fraud, default, we need to study the current Indian landscape of financial technology solutions, their benefits and adoption & supplement it with real time merchant survey of technology adoptions, their benefits and risks. Once we have done this, we can propose solutions (also referencing available research)

II. METHODOLOGY

The proposed methodology will cover 3 step process

1. Study of current fintech model of companies namely Paytm, Mobikwik, and Razorpay and UPI
2. Role of technology in Fintech
3. Survey select merchants on current fintech solutions and analyse their survey feedback
4. Proposed way ahead of the role of technology in identifying willful defaulters
5. Future Scope of Work

We have used research on Fintech models in India with a focus on Paytm, Mobikwik, and Razorpay business models

III. FINTECH MODELS IN INDIA

Fintech (Financial Technology) is a convergence of financial services with digital technologies. Empowered with advanced data & analytics capabilities, zero-processing costs, and asset-light platforms, fintech companies are providing a better, advanced form of financial solutions to their varied clients across industries. E.g. digital transactions, and digital payments, Most of the Fintech companies in India got a digital kickstart thanks to the famous demonetization drive in the year 2016. Moreover, the grand launch of the 'Digital India Initiative' has a big contribution to the transformed landscape of the payment interface of India. Below are the key fintech offerings from various companies

- ***Digital Wallets*** – Paytm, Mobikwik, PhonePe, Google Pay - This model involves an application-based mechanism wherein a user preloads or puts virtual money into wallets for online transactions with businesses who accept this form of digital wallet as their payment mechanism.
- ***Digital Banking*** - is the incorporation of digital tools and technologies for attending to banking chores and activities, customers can have a quick look into a bank account on mobile only).
- ***Payment Gateways***- Fintech companies integrate varied payment methods into the convenient form of applications or apps. These applications are adopted by online merchants, online businesses
- ***Digital Insurance*** - Indian Fintech companies like Policy Bazaar - are changing the landscape of the insurance industry by bringing their traditional mode of insurance services directly to the digital world.
- ***Digital Lending*** –Digital Lending is a striking business model where Banks decided to digitalize the entire lending operations for agriculture loans, and home loans thus reshaping a traditional lending system into digital lending.
- ***UPI - Unified Payments Interface (UPI)*** is a system that powers multiple bank accounts into a single mobile application (of any participating bank), merging several banking features, seamless fund routing & merchant payments into one hood

Fintech companies in India are seeing a massive surge and their value creation opportunity now stands at an enormous 100 billion USD. As part of our research, we will focus on Digital Wallets and Payment Gateways – namely Paytm, Mobikwik, Razorpay and UPI

Paytm Business Model

We refer to Paytm blog of (Prasad Dilip, 2022), to understand in detail the Paytm business model. Paytm was Founded by Vijay Shekhar Sharma in 2010. Paytm business model is – to Drive revenue growth with low Customer Acquisition Costs (CAC) (e.g. UPI) with high engagement payments business and cross-sell financial services products. Key unique features of Paytm are

- **Enabling Financial inclusion** by Offering a comprehensive suite of payment services to acquire consumers and merchants - Widest Range of Payments Services: Like cards, net banking, Paytm Payment Instruments like Wallet, UPI, and Fastag to make online payments for Mobile Recharge, Utility Bills, Rent, Tolls, Education, Wallet top-ups and money transfers using the Paytm app.

- **Leveraging Platform Engagement to Enable Merchant Partners' Growth:** High consumer adoption encourages merchants to join the platform, and also use commerce offerings to leverage consumer traffic to grow their business. E.g. merchant partners can grow their business by offering services like the ability to sell tickets, advertising, and loyalty solutions like deals and gift vouchers.

-
- **Driving Subscription-led Ecosystem for Merchants:** On the merchant side of the platform, Paytm enables partners with tech solutions that allow them to accept payments through a wide variety of instruments and by deploying subscription-based devices that help with reconciliations.
- **Using Two-sided Ecosystem and Insights to Upsell High-margin Financial Services:** enables to upsell high margin and low customer acquisition cost (CAC) financial services to consumers and merchants - small ticket lending products, Personal Loans and Merchant Loans

Problems Faced By Paytm-

1. Competition: Paytm faces intense competition from other players in the Indian e-commerce market.
2. Security concerns: As a digital payments company, Paytm has faced security concerns related to the protection of customer data and the prevention of fraud. The company regularly invests in improving its security measures.
3.

Mobikwik business model

We refer to work of (Kumar, Shubham, 2023), to understand Mobikwik business model better. Founded by the husband-wife duo, couple Bipin Preet Singh and Upasana Taku in the year 2009, to make payments easy and fun for every Indian -wallet and To make personal wallets redundant. The mission of MobiKwik is "to build a world-class payments and credit product for Bharat!" The company was started in 2009 with a vision of "transforming the digital payments landscape in India." MobiKwik is one of the largest mobile wallets in India. It allows Indian consumers to store money in a virtual wallet and then use it across channels (mobile, desktop, tab, SMS, IVR) to pay utility bills and shop all they want. Now it is a full-stack fintech company. One can do bank transfers, and can also take loans. The revenue of Mobikwik comes from the commissions on each transaction that takes place, via partnering with companies and through the advertisements that they consider fit for their app. Furthermore, MobiKwik also gains fee-based incomes by cross-selling insurance and mutual fund products. Mobikwik revenues come from its credit products and payment solutions.

Challenges face by Mobikwik are similar – competition and security challenges.

Data Security –This has been one of the major problems of the company. Company is investing in this area esp. linked to their customer base.

Competitors – There is high competition in the market place in digital wallet space. Mobi Kwik has carved its offerings clearly and continues to develop them over a period of time.

Razorpay business model

We refer to work of (Arangarajan, Abinaya, 2023) to understand Razorpay business model.
Founded in 2014 by IIT Roorkee alumni Harshil Mathur and Shashank Kumar, Razorpay is one of India's leading online payment gateways, offering a range of financial solutions to businesses. Its business model revolves around providing secure and hassle-free payment gateway services to businesses and generating revenue through transaction fees and financial solutions. Along with small and medium-sized businesses, the platform is designed to serve a wide range of businesses across industries. Its platform can be used by multiple business sizes. Razorpay's business model is based on providing online payment gateway services to businesses and charging a fee for every transaction processed through its platform. The company offers two plans to its clients - the Standard Plan and the Enterprise Plan. Apart from transaction fees, Razorpay also generates revenue from its financial solutions like Business Banking Hub, which offers advanced financial management tools to businesses, including payouts, corporate credit cards, and current accounts. Overall, Razorpay's business model is based on providing reliable and secure payment gateway services to businesses and generating revenue through transaction fees and financial solutions.

Challenges faced by Razorpay-

1. Credibilty - most people still lack the trust to rely on fintech to simplify their financial operations. This is again linked to security and potential fraud risk.
2. Customer relationships – As Razor pay has business focused model, maintaining customer relationship is key. Razorpay continues to invest in this area, as it needs to make sure that they retain customers for the long run by building long-term customer relationships.

UPI

We refer to (NPCI) website having product overview of UPI.

Unified Payments Interface (UPI) is a system that powers multiple bank accounts into a single mobile application (of any participating bank), merging several banking features, seamless fund routing & merchant payments into one hood. It was founded by NPCI – the National Payment Corporation of India. With the above context in mind, NPCI conducted a pilot launch with 21 member banks. The pilot launch was on 11th April 2016 by Dr Raghuram G Rajan, Governor, RBI at Mumbai. Banks have started to upload their UPI-enabled Apps on Google Play store from 25th August 2016 onwards. **Its key features:**

- Immediate money transfer through mobile device round the clock 24*7 and 365 days.
- Single mobile application for accessing different bank accounts.
- Virtual address of the customer for Pull & Push provides incremental security with the customer not required to enter the details such as Card no, Account number; IFSC etc.
- Merchant Payment with Single Application or In-App Payments.
- Utility Bill Payments, Counter Payments, QR Code (Scan and Pay) based payments.

Participants in UPI - Payer, Payee, Remitter Bank, Beneficiary Bank, NPCI, Merchants

As it can be seen from above that adoption of digital payment solutions is rapidly increasing, however challenges faced are common around security concern including fraud prevention. All these companies are investing in technology to pro-actively identify planned defaulters. In further work, we outlay how technology can help in this – let us first study role of technology in Fin Tech

Role of Technology in FinTech

We refer to work of (Fong, Dick et al, 2021) and (PwC, 2023) for studying the use of technology in financial technology. Apart from User front and, Back end code, technology has below advanced usages

● **Artificial Intelligence**: By learning and adapting data from data, the models of AI can perform any task without human intervention. It helps get the work done quicker, more efficiently, and more accurately, for example – Chatbot, AI algorithms to avoid fraud,

● **Machine Learning**: Algorithms of machine learning used in finance work in the best ways for the identification of patterns. These algorithms also aid in the detection of relationships among numerous sequences and occurrences. Thereby helping to extract the important data hidden among the massive data sets. The aspect of machine learning in the financial industry also opens the doors to spotting suspicious activities and helping in the best possible ways to prevent fraud. So, ML in FinTech can act as a game changer.

● **Cloud Computing:** The integration of cloud computing enhances security with the help of automated and embedded security controls. It accomplishes the same thing by offering a route for secure data sharing

● **Blockchain:** The potential of blockchain to upend the current banking system is huge. Data may be shared, recorded, and synchronized across several data repositories in real time

● **IoT**: The Internet of Things is a network of physical objects that are embedded with sensors, software, and other technologies. These objects can connect to other devices and systems over the internet and share data with them

We have also conducted a real time survey with 100 vendors (small businesses shops) to identify use of fin tech solutions and the challenges faced.

<u>Survey on Fin Tech use in India with select merchants</u>

A quantitative survey was done with select 100 merchants in National Capital Region (NCR) region across Delhi, Gurgaon with below objectives, methodology

Objectives of Survey

Below are the objectives of the survey -

a. Adoption of Fintech in daily transactions – covering both merchants and customers
b. Benefits and Challenges being faced in adopting Online payment methods
c. Risks involved in Online payment methods and dealing with Fin Tech service providers
d. Response needed from Fin Tech companies in case of Risk / potential fraud

Methodology of Survey conducted

A series of 12 Questions were covered with 100 merchants in NCR region of Delhi / Gurgaon.

- Q1-6 are focused on adoption and benefits of fin tech solutions at merchants including their customers.
- Q7-12 are focused on Risks involved in online transactions at merchants and probable solutions expected from Fin tech companies in case of potential error/ fraud

Survey was conducted using the 12 Questions in hard copy format and seeking merchant responses (100 numbers). The responses were tabulated for results and analysis at completion of survey. Survey was done in month of January 2024.

Survey Outcome and Observations

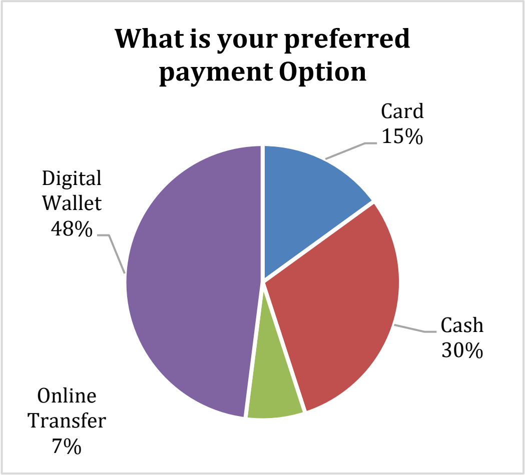
The responses for Q1-6 focusing on adoptions of Fin technology at merchants for day to day business are tabulated as below. The key observations are

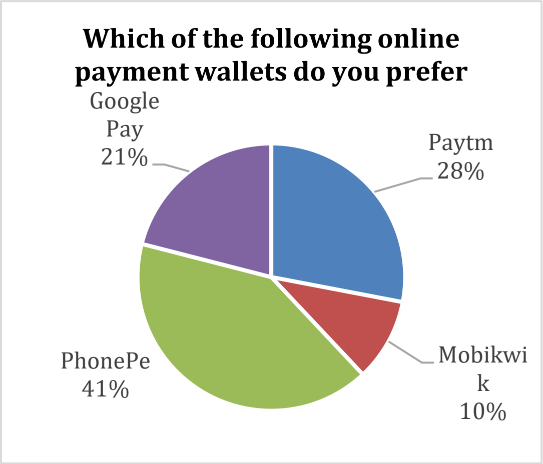
- Very high adoption of Fin tech solutions at Merchants (Digital Wallet & Cards) – Q1
- Phone Pe is preferred option followed by Paytm (driven by fees and ease of use)-Q2
- Both merchants, customers are highly skilled at use of technology (not linked to level of education, fin tech solutions have adopted for all sections and very easy to use– Q3,4)
- >75% of transactions are online (non Cash) – Q5
- Online Fin Tech solutions are preferred due to Higher Sales followed by Ease of use – Q6
-

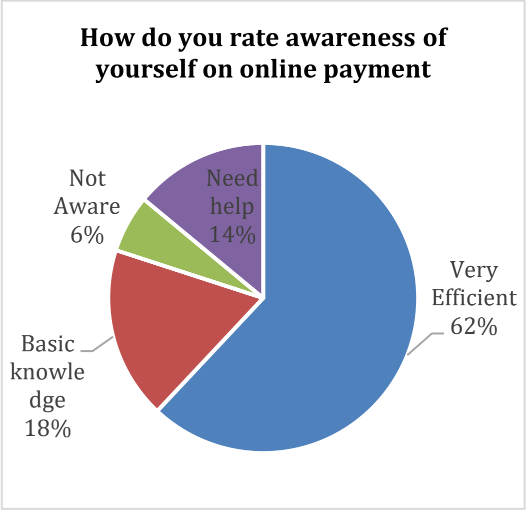
The responses for Q7-12 focusing on Risks of Fin technology at merchants and probable solutions for day to day business are tabulated as below. The key observations are

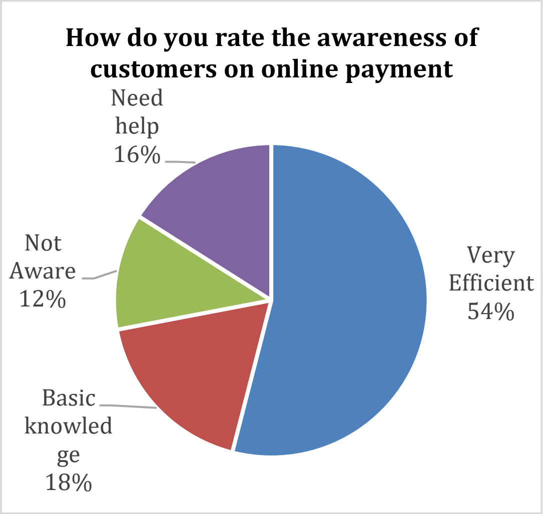
- Fraud Risk is one of the top high risks – Q7
- Merchants are not happy with current response of Fin Tech providers in case of fraud -Q8
- There are significant transactions (>0.1-1%) which are related to errors/fraud -this is important if we have to scale up fin tech further – Q9
- Multiple reasons shared for fraud and errors by merchant – not a single specific reasons: leading to need to all round solutions to tackle fraud – Q11
- Probable solution proposed is Faster response and immediate decline in case of potential fraud and decline (as it takes lot of time to rectify post transaction and leads to merchant/customer dis-satisfaction) – Q10, 12

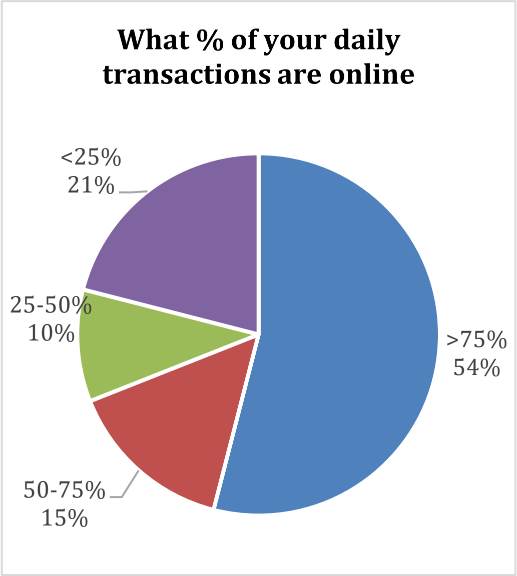
Question 1-6 outcomes (100 sample size) – on Adoption of Financial Technology at Merchants

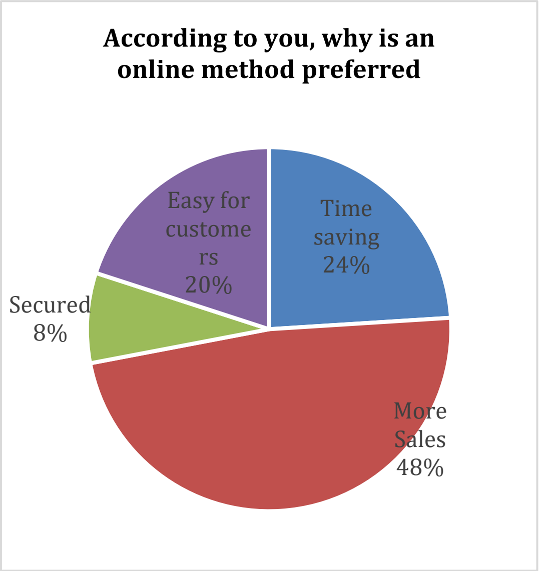




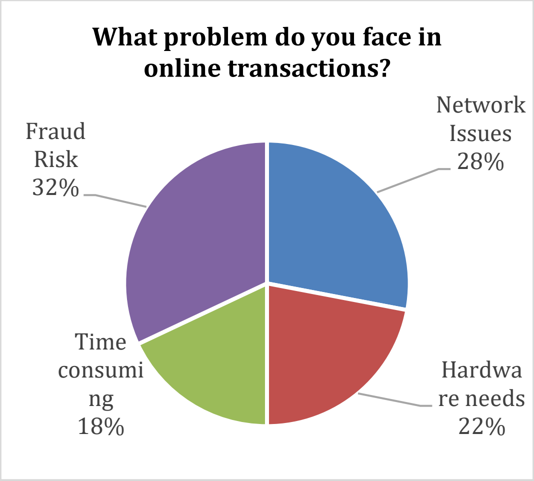


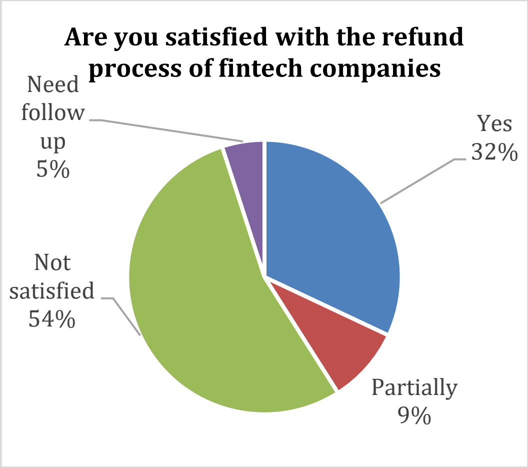


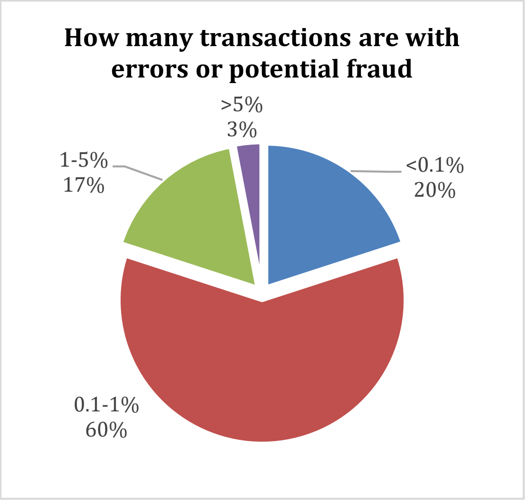


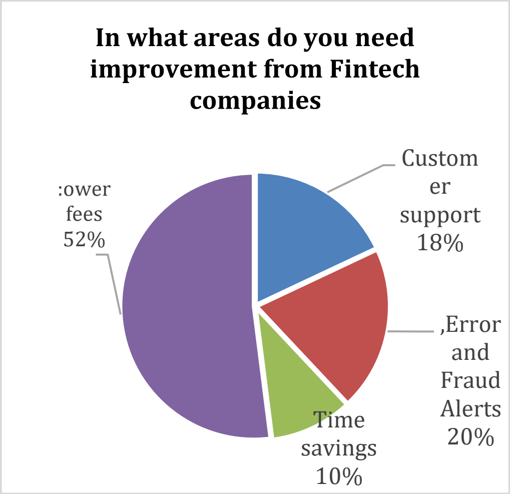


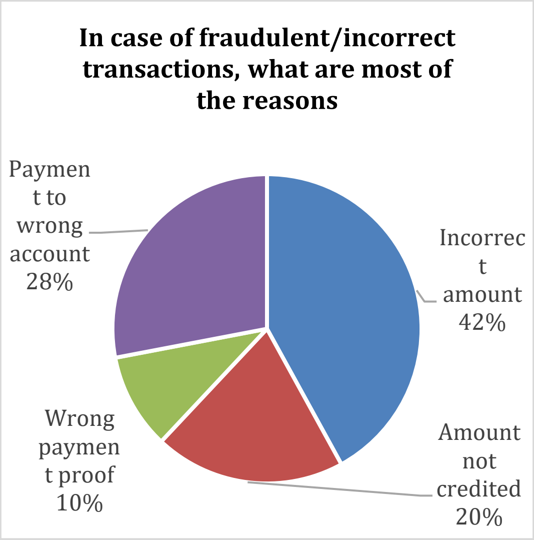
Question 7-12 outcomes (100 sample size) – Trend on Risks of Fin Tech and probable solutions

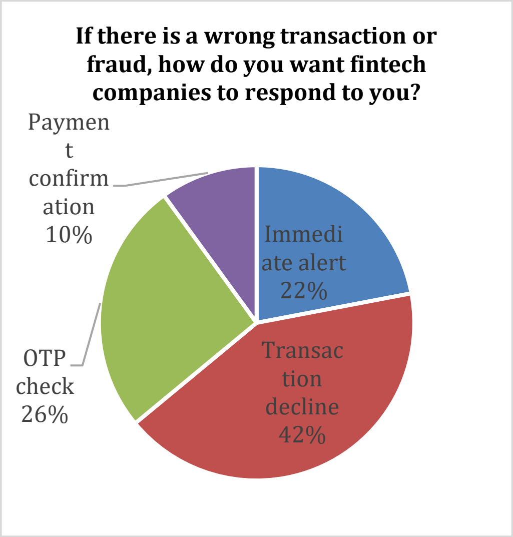

What problem do you face in online transactions?


Are you satisfied with the refund process of fintech companies


How many transactions are with errors or potential fraud


In what areas do you need improvement from Fintech companies


In case of fraudulent/incorrect transactions, what are most of the reasons


If there is a wrong transaction or fraud, how do you want fintech companies to respond to you?

IV. CONCLUSION FROM SURVEY

Below are the conclusions from Survey

- Fin tech solutions are being adopted at fast pace by both Merchants and customers. It is due to ease of use and higher sales. Online Transactions share is increasing and much more than traditional Cash format.
- There are risks related to fraud and errors related to online transactions, this is on increase with rising number of online transactions.
- Merchants are not happy with current solutions in place and needs faster early detection of fraud/error, and faster response from Fin Tech companies
- Online transactions (e.g. Digital wallet) are here to stay and grow. More work is needed to fix and detect the potential fraud.

As speed is important in fin tech solutions for merchants and customers, manual checks are not feasible. Hence Technology will play a big role in addressing this gap. This will be through Artificial Intelligence, Machine Learning (algorithm for detecting fraud) and Coding to address hence solutions. All this needs to happen real time with technology taking decisions on Transaction decline, merchant alert or more checks to complete transactions (like 2nd check OTP). The next section of paper suggest how technology can play part in this area.

Short coming of Survey

Below are short coming of current survey

- Survey has been done in Delhi/Gurgaon region, and hence may not cover entire geographical area of India with other different regional aspects.
- Survey has been done in particular time of January, any seasonal variations are not captured

Even with shortcoming, the findings across 100 numbers are significant for analysis and can be used.

Having studied role of technology in fin tech and also feedback from survey, we can conclude need to use to technology in detecting payment frauds. We detail the same in coming sections.

Role of technology in detecting payment fraud

We refer to work of (PwC, 2022) and (PwC, 2023), (Infosys BPM Newsletter, 2023) and industry research including expert interactions. Let us first study the types of fraud and drivers of fraud. According to the Reserve Bank of India, there were over 13 thousand instances of bank fraud in the current financial year.

Users have multiple options for digital payments such as cards, wallets, UPI, mobile banking, QR code and various other methods. The increase in the adoption of these advanced payment options has also generated unprecedented opportunities for fraudsters to perpetrate fraud by exploiting digital payment systems and human vulnerabilities. PwC study quotes, as per the Reserve Bank of India's (RBI) Annual Report 2021–22, the volume of frauds reported by financial institutions (FIs) using cards and internet banking was 34% higher at 3,596 in 2021–22 as against 2,677 frauds in 2019–20. With the rise in technological advancements, incidents of fraud have also become more organised and sophisticated.

The advanced techniques used by fraudsters impact customer trust in digital payment instruments. Fraud may lead to loss of reputation and huge liabilities. Therefore, it is of utmost importance to mitigate and prevent such incidents. Having risk mitigation measures in place can significantly reduce exorbitant operational costs. Such measures eliminate the need to spend time and resources on reviewing every transaction alert.

We summarise the various types of Fraud as below -

1. **1st Party-Customer is the starter**: An applicant shows altered or incomplete information that alters the underwriting decisions or terms . Here, the customer is leading to fraud and is also doing the authentication.

2. **3rd Party-Customer is the victim:**_Here, customer is not creating the fraud._Customer's online profile or account information is hacked. Fraudster withdraw funds without customer's knowledge . This can be done by fraudster through getting customer sensitive information(login credentials , account details) via text messages ,email etc. Authentication is done by the fraudster.

3. **Identity Fraud** :In this also, customer's personal information is stolen. customer's is impersonated in a bank branch or over phone, an account is made in the customer's name; hence it is a false identity created.

4. **Account Takeover :** In this username/ password of the customer become compromised, automatically through online downloads (Malware - Customer downloads malicious software).

5. **Phishing**: The customer is scammed into providing account details , authentication credentials , access to the device to an individual typically via phone interaction . Authentication may be passed by the fraudster or customer.

- Fraud increase can be attributed to
- Diversified entry points
- Vulnerabilities in the new payment technologies
- Lack of customer awareness
- Unsecured remote access

Common fraud techniques used in an Indian context, including common tactics used by fraudsters

- Identity theft/impersonation
- Phishing/vishing
- Web skimming
- By using QR code
- Account takeover
- Database breach

Some of the payment channels used by fraudsters are listed below:

UPI payments and wallets - Many fraudsters create UPI handles with a valid-looking or genuine-appearing name, such as 'BHEM'/'BHEEM' or 'NPIC', to deceive the user, who believes these handles to be authentic and disclose their account details. Most UPI frauds are driven by users' ignorance and lack of awareness of the platform.

..

ATMs /point-of-sale (PoS) machines - By using personal data obtained via remote access assistance or skimming devices installed at ATMs/POS machines, fraudsters execute transactions from the user's account.

Internet banking - Using confidential data such as login credentials obtained through various fraud methods like phishing or remote access assistance, fraudsters execute illegitimate Internet banking transactions.

Mobile banking - With an increase in the availability of smartphones and internet penetration, mobile phones have become the most opted instrument to perform digital transactions. However, as such channels are vulnerable to fraud, the fraudsters can misuse the user's credentials or personal data to penetrate the user's banking application.

Having reviewed the methods used by defaulters, we now study how this can pro-actively managed.

Fraud Management

Below are some of the key areas through which Fraud can be managed. We need to adopt a framework that integrates the people, policy and process, and technology aspects for a more effective, agile and dynamic anti-fraud response.

Banks use a program called KYC(Know your customer).Before giving any loans, the banks must get to the know person/institution they are lending loan to, that is their name, PAN/Adhaar number, prior loans taken, and their bank account balance.

- The **people aspect** emphasises the importance of the human aspect in the operationalisation and implementation of a robust fraud risk management framework (training and awareness)
- The **process aspect** emphasises the tone at the top — which refers to the commitment of the top management towards robust fraud risk management policy —and enables a strong, anti-fraud response by setting up strategies, policies and procedures
- The **technology aspect** plays a key role in the implementation of a strong fraud risk management framework by using the right technology and tools for fraud prevention and detection.

Effective fraud management strategy requires a fine-tuned balance between preventing fraud, limiting costs of implementation and maintaining a positive customer experience. Below are few ways to limit the fraud.

Identity fraud can be managed by verifying customer's identity during account maintenance or identity screening.
Check fraud can be managed by advanced customer authentication. Advanced customer authentication can include OTP verification ,alert/confirmation messages for transaction etc.
Account Takeover fraud can be controlled by login device verification e.g. password check or multi factor authentication OTP messages , alert messages seeking permission can be sent to the customer . If the account is taken over , the account can be temporarily freezed.

We now specifically focus on role of technology in fraud management. We refer to (Infosys BPM Newsletter, 2023). Technology plays a vital role in financial fraud detection. With the continued growth of e-commerce and digital payment systems, fraudsters are becoming more adept at exploiting vulnerabilities in these platforms. Combating retail fraud has become especially challenging due to the sheer volume of transactions processed daily. For example, artificial intelligence can analyze large amounts of data for suspicious activity.

Encryption: Blockchain technology can secure, monitor, and track changes to financial transactions in real time. You can control who has access to data and see the changes they have made to identify and prevent fraud from happening. People nowadays use digital payment methods as it is easy and cheap (UPI). If they are making a transaction, to check whether they are the only ones making a transaction there can be two levels of security check:

1. First level security check: While making the transaction they can use the OTP check, wherein before making the transaction OTP would be sent to that person. The person would be notified about the transaction and can decide whether to approve it or alert the authorities.
2. Second level security check: If the transaction is a huge amount or of greater than the usual trend of transactions done by the person, the bank will be notified. Then a call would be made from the bank to the customer, getting their consent and then approving the payment.

Machine learning algorithms to detect suspicious activities: These sophisticated algorithms diligently analyse transactional data to detect any anomalies or outliers that might indicate fraudulent behaviour. By continually adapting and learning from new data, the system proactively identifies emerging fraud tactics and stays one step ahead of fraudsters. This adaptive capability ensures ongoing refinement and optimisation, enabling businesses to effectively combat evolving fraud threats.

Machine learning algorithms are used when we are dealing with a huge set of data. We can put the data in the machine, it would identify the patterns in the data and help in classifying the defaulters. Patterns can be like a particular nationality belonging to this region, occupation etc are defaulters. So the bank will not lend the money to them.

Coding: If they are capable of the loan can easily track their bank account balance using coding. They can have a primary key(which has the person's name and their PAN number as a combination), and they can track the person's bank balance using this and see if they are eligible for the loan or not.
Coding ensures-Speed of checking manually whether the person can be a potential defaulter or not, we can use coding. Doing this manually can be tiresome and can take days to check. Coding makes this task easier and quicker. We can put a set of conditions like for this category/occupation/nationality/salary etc if their budget is greater than a fixed amount we can lend them else no.

Accuracy-Coding makes this a lot more accurate, it reduces the chances of error. Doing manually increases the chance of human error, the information can be misread or copied wrong but in coding, we have already classified the conditions and it makes it easier for us to check. We can easily add new conditions to our existing code to classify a person as a defaulter thereby making the identification. Ore is accurate.

Transparency-There exists a central database which contains information about the person's bank account transactions and balance. Via coding, this information can be made available to all the banks. All they need to do is enter the primary key and all information would be made available, making it easier to classify him as a defaulter or not.

The sophisticated technology analyses transaction data and raises a red flag whenever it identifies unusual patterns, thereby effectively reducing the risk of fraud. Additionally, some retailers can opt for tamper-resistant terminals designed specifically for credit cards, further safeguarding their business from credit card fraud. By integrating such robust technologies, retailers can protect their business and instil consumer trust and confidence at the point of sale. This enhanced customer experience not only bolsters customer loyalty but also attracts new customers who prioritise security and peace of mind.

Future trends in retail fraud prevention technology
As fraud tactics continue to evolve, so too do the technologies deployed to counter them. Some trends expected to shape the future of retail fraud prevention technology include:

- Enhanced machine learning and artificial intelligence capabilities, providing more accurate predictions and quicker detection of fraudulent activities.
- Biometric authentication methods add an extra layer of security for customer verification and authentication. Before making any transaction the app which we use for payment can ask us for our fingerprint scan. The sensors will match the pattern and then proceed further.

To add security further, while making an account on the digital platform for payment, we would be asked to upload our photo. There should be no obstructions like the face should not be covered, the lighting should not be too dim or bright, and the picture should be clear. Also to avoid robot intervention, questions can be asked or there can be sensors to detect any robotic presence. If detected, system can be triggered and then an account cannot be made. So before making any transaction on that platform, the camera sensors can use a face recognition system.

V. CONCLUSION

Had these technologies been there earlier Shubhangi, Sushma and many others like them wouldn't have lost their money. Technology could have aided in identifying the exact location of duped people, dupester, and during the time taken by fraudsters to make transactions – identifying

the potential fraud attempt, sending a second OTP would have made a huge difference in preventing fraud and thus could have helped in preventing their losses financially, emotionally and mentally.
We are sure that fin tech companies will adopt above solutions in technology for pro actively identifying planned defaulters, which will help further increasing adoption of digital payment solutions across in safe and secure way.

VI. BIBLIOGRAPHY

Andreeva, Ansell, and Crook (2007)
Galina Andreeva, Jake Ansell, Jonathan Crook, "Modelling Profitability Using Survival Combination Scores.", *European Journal of Operational Research*, North-Holland, 13 Jan. 2011, www.sciencedirect.com/science/article/abs/pii/S0377221706011921 , Accessed 8 Jan. 2024
Arangarajan, Abinaya, 2023
Arangarajan, Abinaya. "Business Model of Razorpay: How Does Razorpay Make Money?" *StartupTalky*, 28 Mar. 2023, www.startuptalky.com/razorpay-business-model/, Accessed 10 Jan. 2024.
Crook et. Al, 2007
Jonathan N. Crook, David B. Edelman, Lyn C. Thomas. "Recent developments in consumer credit risk assessment", *European Journal of Operational Research*, North-Holland, 13 Jan. 2011, https://www.sciencedirect.com/science/article/pii/S0377221706011866, Accessed 9 Jan. 2024
Fong, Dick, et al, 2021
Dick Fong, Feng Han, Louis Liu, John Qu, and Arthur Shek, et al. "Seven Technologies Shaping the Future of Fintech: Greater China." *McKinsey & Company*, 9 Nov. 2021, www.mckinsey.com/cn/our-insights/our-insights/seven-technologies-shaping-the-future-of-fintech. Accessed 11 Jan. 2024.
Infosys BPM Newsletter, 2023
"How to Detect and Prevent Banking Fraud?: Infosys BPM." *Infosys*, www.infosysbpm.com/blogs/bpm-analytics/fraud-detection-prevention-banking-sector.html, Accessed 11 Jan. 2024.
Kumar, Shubham, 2023
Kumar, Shubham. "Mobikwik Success Story - Business Model: Founders: Revenue: Funding." *Startup Talky*, 29 Nov. 2023, www.startuptalky.com/mobikwik/, Accessed 11 Jan. 2024.
Liu, Fan et. Al., 2014
Fan Liu, Zhongsheng Hua, Andrew Lim. "Identifying Future Defaulters: A Hierarchical Bayesian Method." *European Journal of Operational Research*, North-Holland, 13 Aug. 2014, www.sciencedirect.com/science/article/pii/S0377221714006432#b0045, Accessed 10 Jan. 2024.
NCPI
"UPI: Unified Payments Interface - Instant Mobile Payments: NPCI." *National Payments Corporation of India (NPCI)*, www.npci.org.in/what-we-do/upi/product-overview, Accessed 10 Jan. 2024.
Prasad, Dilip, 2022
Prasad, Dilip. "Our Business Model Explained – Driving Revenue Growth through High Engagement Payments Business and Cross-Selling Financial Services" *Paytm Blog*, 17 Aug. 2022, www.paytm.com/blog/investor-relations/our-business-model-explained/, Accessed 11 Jan. 2024.
PwC, 2022
PricewaterhouseCoopers. "Combating Fraud in the Era of Digital Payments." *PwC*, May 2022, www.pwc.in/industries/financial-services/fintech/dp/combating-fraud-in-the-era-of-digital-payments.html, Accessed 14 Jan 2024
PwC, 2023
PricewaterhouseCoopers. "Artificial Intelligence and Its Role in the Fight against Fraud." *PwC*, 15 Jun. 2023, *PwC*, https://www.pwc.com/mt/en/publications/other/artificial-intelligence-role-in-the-fight-against-fraud.html, Accessed 14 Jan 2024