DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

PayPal

Fraud & Risk Management in Digital Payments

A DSCI-PayPal Joint Study

Table of Contents

Foreword: DSCI-PayPal

With the rise in Digitization, comes ease of transactions but also mushrooms a growing threat landscape. India has been riding on the back of digital uprising and huge investments in the Fintech sector to revolutionise the payment sector.

The growth of India's digital economy owes a large part of its success to RBI, NPCI, Government of India's less cash vision in enabling multiple retail payment systems introduced in the last few years, including Unified Payments Interface (UPI), Aadhaar Enabled Payment System (AePS), Immediate Payment Service (IMPS), National Electronic Toll Collection (NETC) and RuPay Cards, among others.

In July 2020, UPI transactions in India have crossed 1.49 bn in volume and USD 41 bn in transaction value[1]. This coupled with an increase in smartphone penetration and mobile internet access has made India, one of the fastest growing countries adopting Digital Payments in the world. The positive momentum is enabling payment providers to offer personalized experiences that are seamless and user centric and driving digital payments acceptance by consumers and MSMEs. Another important aspect to keep in mind is security and fraud protection as India is rapidly growing share in cross border retail transactions and plans for UPI & RuPay to scale internationally in the years to come.

However, this has led to an escalating fraud scenario with fraudsters coming up with new mechanisms to perpetrate fraud using the same innovations to their advantage by attacking businesses and end users. Among the many new type of emerging frauds, few include buyer side frauds – fraudulent claims, chargebacks, fake buyer accounts; merchant side frauds – selling counterfeit, non-fulfilment; cyber security frauds – account takeover, identity thefts, etc.

On the technology front, the e-commerce and traditional retail sector has been constantly leveraging emerging tools and technologies such as AI, ML, Computer Vision, conversational AI, Data Science and NLP to redefine customer engagement and minimize risks, but they aren't immune to new threats emerging by the day.

The report provides a detailed overview of India's retail payment ecosystem, various kind of frauds, associated risks and case studies, laws in India to fight payment frauds, grievance redressal models in place, and recommendations for involved

[1]UPI Product Statistics; NPCI; July 2020

stakeholders. The need of the hour is to find a right balance between technology enablement, vis-à-vis fraud prediction, and prevention with seamless user experience.

While the Government is committed to establish latest ICT infrastructure and services to deliver safe citizen centric e-services, the ever-growing threat landscape warrants collaboration from Fintech players, payment providers, LEAs to join hands and come up with resilient solutions to minimize risk for MSMEs and consumers.

This report, a partnership between DSCI and PayPal, is a joint endeavour to bring forth the current Digital Payment fraud and risk management scenario and initiate discussions towards real-time fraud prevention strategies. The report also seeks to highlight the vital aspect of collaboration between LEAs, Industry and Govt. regulators and sustained need for digital literacy and Digital suraksha programme for consumers and MSME community to enable a sustained and secure growth to achieve goals of Less cash society and Digital India.

We shall be further working together to build capacity in the form of workshops, curated content, pocket handbooks to alleviate the current risk scenario and spread awareness. We hope this report serves our stakeholders in their deliberations to focus on the risk scenario and work together to come up with robust policies and framework for securing and growing India's Digital Payment momentum.

Rama Vedashree
CEO, DSCI

Nath Parameshwaran
Director, Corporate Affairs, PayPal India

Foreword

Rapid digitization has always been one of the core objectives of Government of India. Government initiatives such as Digital India have played a significant role in ensuring that India progresses towards digital economy and becomes a digitally empowered society. The year 2020, with the pandemic gripping the world, has certainly boosted the adoption of digital technologies in every facet of our lives, including Payments. This is true not just for individuals, but also for Small and Medium Business (SMB) communities. Within last 3 months, digital payment platforms across India have surpassed the transaction volume[2], that Experts believed could have taken about five years under pre-pandemic circumstances.

Unfortunately, India has also witnessed a sharp rise in online payment frauds, especially due to increase in the overall attack surface. There is an increase in the percentage of malware campaigns employing COVID-19 related attack vectors. Some of the examples include phishing emails that contain malicious attachments or links, online meeting invites with intention to steal the user credentials, phishing through SMS and increase in number of malicious mobile apps. In May 2020, CERT-In issued alerts around rising Phishing activities in India, especially via fake apps, impersonation and fake websites.

Even though Government of India has taken many steps to support organizations across various sectors in their digital journey, SMB community needs more attention during their digital transformation. The SMB community is still in a very nascent stage of Cyber maturity to handle the current rising threats. Hence, the overall rise in digitization and threats in India requires various stakeholders including Government, Industry leaders, Law Enforcement Agencies to come together to ensure robust cybersecurity posture, especially around digital payments. This cross-collaboration would enable regular interventions to combat the rising cyber threats.

It is heartening to see that DSCI and PayPal have collaborated on this report that highlights the existing legislations in India, types of frauds, key challenges around fraud detection, enforcement, investigation and risk management in online payment industry.

I wish that India becomes a digitally secure nation in its march towards economic prosperity.

Lt. Gen (Dr) Rajesh Pant
National Cyber Security Coordinator, GoI

[2]Virus boosts digital payment in India; The Economic Times; July 2020

"Indian Digital Economy is booming with 90% consumers expected to use digital payments in coming years. The volume of online transactions is expected to exceed USD 500 bn between 2019 and 2023. It is a testimony to Digital India's vision of harnessing growth among small & micro players as well as consumers across India. India needs to contain cyber risk & fraud and build trust in the digital transaction ecosystem which is pivotal to the growth of Digital Economy in the country. It is heartening to see collaboration between FinTech companies, Law Enforcement Agencies (LEA) and payment providers to make all-out efforts to contain the spawning cyber threat landscape that is threatening India's digital payment ecosystem."

Dr Rajendra Kumar
Addl. Secretary, Ministry of Electronics & Information Technology, GoI

EXECUTIVE SUMMARY

Executive Summary

Digital Payments are ubiquitous in today's connected world and have eased payments and transactions. In India, its immense growth can be attributed to technological advancements, Internet penetration, mobile phone uprise, online payment adoption by consumers, SMBs, banks alike, innovative solutions such as UPI, IMPS, wallet integration, etc., and presence of conducive environment by policy makers and Government to transform India into a less cash economy.

However, the threat landscape has also grown dynamically as an unintended effect of the progressive momentum. This warrants attention from all stakeholders involved in the payment ecosystem to join hands and curb the growth of frauds and payment scams. This joint study is an attempt to address the emerging concerns and underlying causes.

The report attempts to discuss about the sophisticated online payment frauds, the threats in the payment ecosystem, the importance of incorporating better fraud prevention strategies and recommendations for various stakeholders involved in the payment ecosystem.

Current Growth Scenario

- E-commerce market is expected to grow to USD 200 bn by 2026 from USD 50 bn in 2018.
- The internet userbase is expected to grow to 835 million by 2023 from 560 million in 2018.
- Growth of online shoppers is 73% for tier-I and staggering 400% for tier-II and tier-III cities.
- 925 million and 47 million debit and credit cards have been issued respectively, as of March 31, 2019.
- Inline Digital India's vision, Digital payments have been on an accelerated growth path over the last several years with NPCI's UPI alone clocking 1.49 bn in volume and USD 41 bn in transaction value, in July 2020.
- MSME's adopting digital channels and transformation have grown twice as compared to their peers using traditional approaches but at the same time remain quite vulnerable to cyber security threats.
- The retail sector is increasingly looking to leverage advanced AI technologies like machine learning, computer vision, conversational AI, Data Science and NLP to bring out better user experience.

Types of Fraud

The e-commerce transaction process entails multiples entities at different stages, such as marketplace, merchants, payment gateways, financial institutes, apart from the consumers and each stage/entity can act as a vulnerability or attack point for malicious actors. E-Commerce frauds can be broadly categorised into:

Buyer side frauds	Fraudulent claims, chargebacks, fake buyer accounts, promotion/coupon abuse, etc.
Merchant side frauds	Selling counterfeit, non-fulfilment, etc.
Cyber security frauds	Account takeover, identity theft, card detail theft, triangulation fraud, etc.

Key Challenges

- Fraud detection, enforcement, investigation and legislative challenges
- Lack of multilevel awareness
- Cross-industry or expertise collaboration
- Security is seen as a cost overhead and not essential investments by stakeholders
- Privacy laws
- Organised criminal involvement

Fraud Prevention Measures & Upcoming Technologies to the Rescue

- **IP Geolocation** to verify consumer's data to determine location at the time of purchase
- **Rules Engines** to allow merchants to create rules that will be evaluated on orders as they come such as 'decisioning software', 'order management'
- **Proxy IP address detection** for instant detection of anonymous IP addresses
- **Machine Learning** for real-time insights and predictive capabilities to detect the fraudulent behaviour instantly
- **Automated Workflow** to speed up payment fraud checks, blocking suspicious devices, fulfilment and cancellation of fraudulent orders, etc.
- **Insights Dashboard** such as reports on suspicious activities in a single interface facilitating the entire fraud screening process immediately
- **Device Fingerprinting** to stop frauds at its root, based on device fingerprints from browser and operating system to language and location

Future Fraud Possibilities

Spoofing of current fraud prevention & detection mechanisms which rely on control parameters like location information; device identifiers like IMEI, MAC address; goods/services identities like SKUs/Barcodes

Exploitation of supply chain vulnerabilities at system & human process interchange

Exploiting risk transfer controls like buyback, insurance settlement of earlier transactions

Recommendations

In order to safeguard payments, the onus lies on every shoulder to mitigate risks and incorporate better fraud prevention strategies. Below are few controls which can be implemented by the various stakeholders involved:

Retail Industry: Should perform regular risk assessment, threat monitoring, advanced data analytics, compliance to standards & audits, open to cross-industry collaboration, additional verification for high value transactions, regular employee and customer awareness, and incident response mechanism in place.

Payment Industry: Adopt security & privacy first culture with commensurate investments in cyber security, adopt security and privacy by design principles at the time of product development (for inhouse, 3rd party vendors and service providers) to mitigate issues at foundational level, consider implementing private/public bug bunny programmes to encourage developer community to find security exploits or vulnerabilities in their infrastructure.

Policy Makers/Regulators: Audit payment processes, standards development, threat modelling, improve laws & legal ecosystem, engage with global partners for skill & threat information exchange.

Law Enforcement Agencies: Empower and upskill prosecution, continuous payment industry training, industry interaction, engage with global LEAs, sensitize LEA on PII, Privacy and data security controls in the payment industry.

Consumers: Never share credentials (OTP, PIN, CVVs), use multifactor authentication, always use licensed and trusted software & devices, use endpoint security like antivirus and firewall, allow only required permissions to apps, use caution while installing apps, be wary of shopping from unknown sites/apps, beware of phishing & other scam methods, learn & share knowledge.

01
INTRODUCTION

Introduction

> India is witnessing a surge in the online payment systems and mobile wallets. These have now started competing with point of sale (PoS) and other traditional methods for payments made in e-commerce transactions.

With the push for Digital India by Government of India, payment systems and wallets are now acquiring more users and there is growth in the number of transactions. Ease of transactions and offers are attracting more users to online retail. Consumers can order services or purchase products, and have them delivered at doorsteps of office or home with just few clicks (or voice commands) on their mobile phones or web. As a result, the Indian financial system has leapfrogged the use of cards and moved to e-payments in large numbers. The Reserve Bank of India in its vision document "Payment & Settlement Systems in India: Vision-2021" predicts the number of digital transactions to increase from INR 2069 cr in December 2018 to INR 8707 cr in December 2021[3]. These predictions would bring further innovation and entry of new players offering optimal cost to the customers and integration of multiple payment systems.

The most straight-forward approach to have a digital push would be to target the generation which is most responsive to technology and digital age. India has a large population of Millennials or Generation Y (individuals born between 1982 and 2004). This generation is also ready to try out new payment systems/channels as long as the rewards are good. India is now at an inflection point with a population of 1.2 billion, of which about 800 million is in the working age. By the year 2026, 64.8% of India's population would be in the working age of 15-64 years.[4]

Retail payment systems and instruments play a key role within both the financial system and the rest of the economy. The committee on payments and market infrastructures noted that "retail payment systems and instruments are significant contributors to the broader effectiveness and stability of the financial system,

[3]Payment and Settlement Systems in India: Vision – 2019-2021, Reserve Bank of India

[4]Engaging Indian Millennial @workplace

contributing to consumer confidence and to the functioning of commerce. Moreover, efficient and safe use of money as a medium of exchange in retail transactions is an essential function of the currency and a foundation of the trust people have in it. For these reasons, the efficiency and safety of retail payments are of interest to central banks.[5]

Consumers are attracted by the convenience, competitive prices and personalised experiences offered by online retail. Higher digital transactions have given rise to the increase in the attack surface, giving rise to the digital frauds.

Consumers using online retail and payment options in India are not new to frauds. Apart from individuals being defrauded, several cases of large-scale frauds and data breach impacting several thousands of users have occurred.

With huge amount of data related to card information that is stored and transferred online, the criminals try to exploit the weaknesses and gain access to this information. With the reports of fraud incidents at different scales at the national and global levels, the consumers have serious concerns over security and privacy. Integrating additional layers of security would have significant impact on the ease of performing transactions by consumers.

The efficiency levels of India's payment systems as published by the Reserve Bank of India in the report titled "Benchmarking India's Payment Systems" published in June 2019, summarises the following:

- The scope of regulation in India extends to the whole gamut of payment systems, instruments, costs and services provided by banks and non-banks.
- The relatively high level of cash in circulation offers scope for higher level of digitisation of payments.
- The growth in the volume of payment systems transactions has been strong and steady.
- Credit and debit cards are growing at a steady rate.
- Strong large value and fast payment systems are in place.
- e-Money growth and options of alternate payments are available.
- Digital communications infrastructure in the form of a robust mobile network is growing strongly. Broadband infrastructure, however, lags in comparison.

Fin-CERT is another umbrella certification for the financial sector in India. As an independent body, it closely ties up with financial sector regulators and stakeholders on issues of cyber security including digital payments. Additionally, the Reserve Bank of India also established a 'Central Payment Fraud Registry' to track frauds in payments systems and monitor digital payments-related frauds on a real-time basis. This was a significant step in preventing and reducing the incidence of frauds in the ecosystem.

This report attempts to discuss about the sophisticated online retail frauds, the threats in the payment ecosystem and the importance of incorporating more sophisticated fraud prevention strategies. Recommendations at various levels are furnished at the end of this report.

[5]CPMI – Non-banks in retail payments; Bureau of Indian Standards; September 2014


24 HOUR ASSISTANCE
9876
123

02
ONLINE DIGITAL SPACE

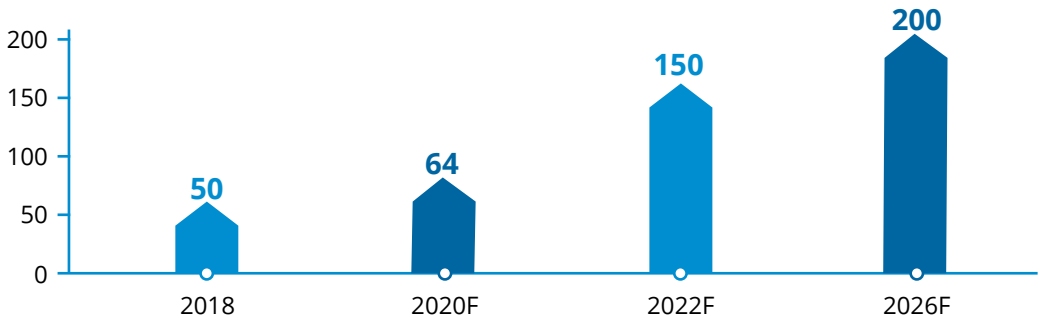
Online Digital Space

2.1 Current scenario – Market dynamics and technology adoption

The internet and digital revolution triggered the e-commerce marketplace in India during the late 90's, soon after the internet revolution began. The e-commerce industry expanded to online retail space covering products from electronics to fashion and travel to groceries. New ventures and fresh investments advanced the online sales over the decades. This coupled with increase in smartphone sales and penetration of mobile internet made the online retail space one of the fastest growing industries in India.

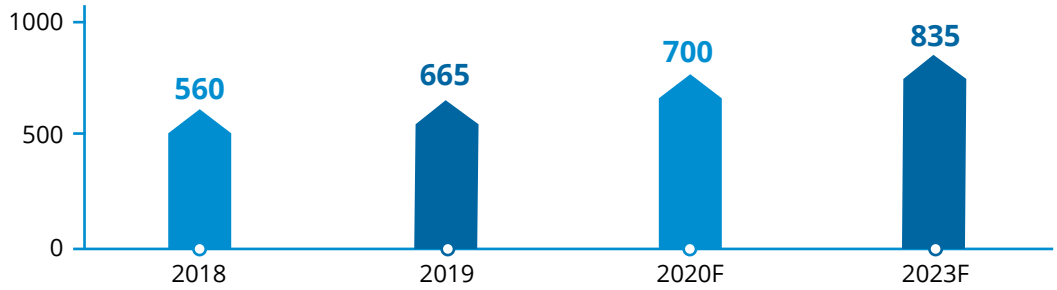
The e-commerce market in India was at USD 50 bn in 2018 and is expected to grow to USD 200 bn by year 2026[6]. India is also adding close to 10 million active internet users every month. Most of these are on mobile and 9 out of 10 users are accessing content in native language.

India E-commerce Market (USD billion)



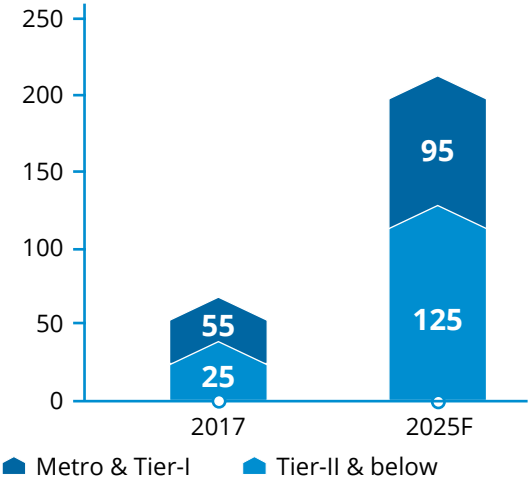
[6]E-Commerce, IBEF; October 2019

Internet Users in India (million)



The internet user base is expected to grow to 835 million by 2023 from 560 million in 2018[7]. Government initiatives like "Make in India" and "Digital India" have pushed the adoption and use of online retail further.

Online Shoppers in India (million)



India is far ahead of developed countries like the UK and the US in adopting mobile payments. The growth of online shoppers in India is at 73% for tier-I and metro cities, while this growth is staggering 400% for tier-II and tier-III cities. This growth rate is because of the wide adoption of digital payments and internet availability. Digital payments in all areas of online transactions including B2B and B2C have considerably picked up despite India being a cash-obsessed economy. Adoption of card schemes like Visa, RuPay, MasterCard for credit and debit cards, online and mobile banking, and inter-bank transfer platforms like UPI, IMPS, NEFT by financial institutions have largely aided the Indian e-commerce growth.

India has attracted investors from across the world to invest significantly in the e-commerce space. New companies have entered the Indian market due to an increase in the investments in the e-commerce sector and are exploring various ways to expand their presence. Currently, the marketplace is a mix of large

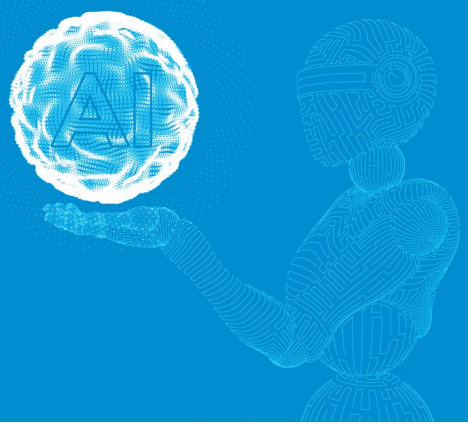
[7]E-Commerce, IBEF; October 2019

e-commerce players like Amazon, Flipkart, Snapdeal, Paytm. Some of the examples of recent[8] changes in market dynamics are as follows:

- In August 2019, Amazon acquired 49% stake in a unit of Future Group.
- Walmart acquired Flipkart paying USD 16 bn for an initial stake of approximately 77% in Flipkart, formally Flipkart Private Limited[9].
- Jio Platforms Limited, a subsidiary of the Company, signed binding agreements with Google International LLC pursuant to which Google would invest INR 33,737 cr for a 7.73% equity stake in Jio Platforms Limited[10].
- Reliance will invest USD 2.86 bn in telecom business to expand its broadband and e-commerce presence to offer 5G services.
- In September 2019, PhonePe launched super-app platform "Switch" to provide a one stop solution for customers integrating several other merchant apps.

On the technology front, the retail sector in India has been constantly leveraging the advanced AI technologies like machine learning, computer vision, conversational AI, Data Science and NLP[11].

- **Conversational AI**: Voice-bots and chatbots to augment customer experience and pre & post purchase engagement
- **Machine Learning**: ML algorithms create models and simulations that predict output based on multiple variables such as sales, weather, location, etc.
- **Data science**: Develop recommendation engines by analyzing customers online as well as offline behavior and preferences
- **Natural language processing**: Handle conversations and provide responses to queries raised by users on the system and external interfaces
- **Computer vision**: Tag objects, monitor human actions and analyze human object interaction to generate consumer behavioral insights



[8]E-Commerce, IBEF; July 2020

[9]Walmart to Invest in Flipkart Group, India's Innovative eCommerce Company; Walmart Corporate

[10]Disclosure under Regulation 30 of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015-Investment into Jio Platforms Limited; July 2020

[11]AI pervasiveness in Retail; NASSCOM; January 2020

2.2 Frauds and risks in financial sector

Fraud can be defined as an act or omission which is intended to cause wrongful gain to one person and wrongful loss to the other, either by way of concealment of facts or otherwise. Earlier, the criminals were more interested in compromising a target by denial of service or website defacement. Today they have graduated for profiting through payment cards or stealing Personal Information, data breaches, ransom, or nation-state warfare.

Under the Indian Penal Code (IPC), a person is said to do a thing fraudulently, if he does that thing with an intent to defraud. The IPC defines and prescribes punishment for various acts that may lead to the commission of fraud.

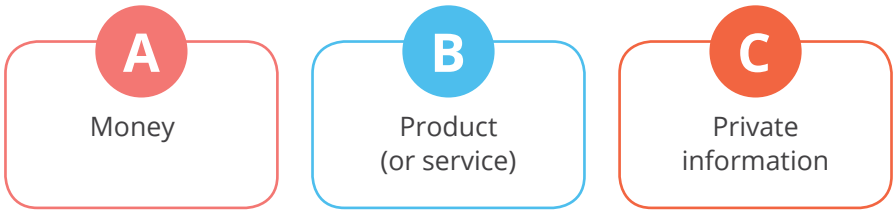
Under section 17 of the Indian Contract Act, 1872 "Fraud" means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto of his agent, or to induce him to enter into the contract:

- The suggestion, as a fact, of that which is not true, by one who does not believe it to be true;
- The active concealment of a fact by one having knowledge or belief of the fact;
- A promise made without any intention of performing it;
- Any other act fitted to deceive;
- Any such act or omission as the law specially declares to be fraudulent.

The Reserve Bank of India (RBI) mentions fraud as "a deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank".

Fraud can be categorized based on two parameters – Impact and the cost

Impact: It is essential to understand the end objective of criminals committing financial frauds. It is difficult to single out the reason behind fraud, and depends on various factors like motivation of the criminals, technical capability of the fraudster, perceived suitability of targets for fraud and actual consequences of discovery. They intend to obtain any or all the below:



Cost: The cost of any cyber security breach on an organisation or financial system cannot be determined immediately as we would never know what the criminals would be doing with the data that is harvested.

- The criminals may use the stolen data for purchases of goods and services or use it for any other purposes

- The proceeds may be used to fund any criminal or insurgent groups
- Purchase of illicit material using the stolen credential
- The proceeds may be put through certain money laundering or round tipping processes to legitimize the funds

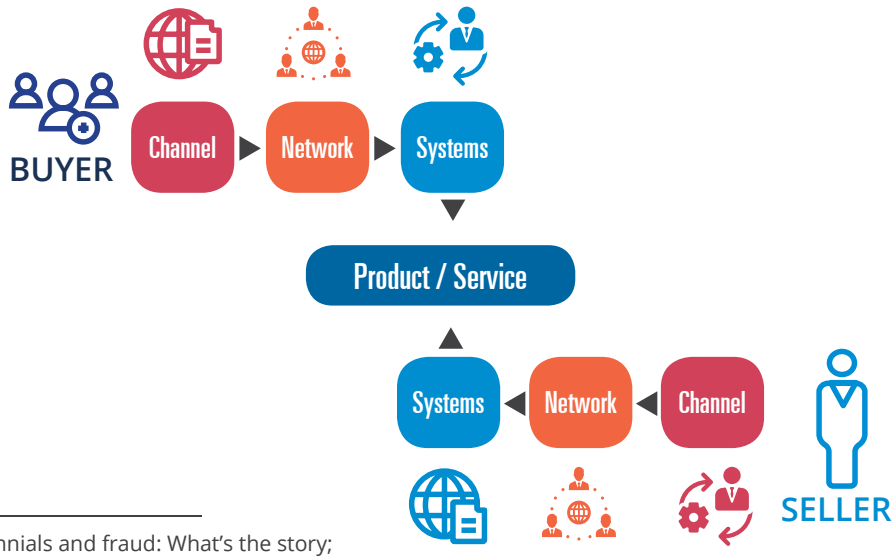
The repercussions of frauds are very serious in nature and may affect both the merchants and consumers. For example, chargeback fees from the issuing bank, negative buzz on social media about the company's reputation, etc.

A report[12] by the Federal Trade Commission (FTC) has revealed that millennials are 25% more likely to report losing money to fraud than consumers ages 40 and over. The FTC's latest Consumer Protection Data Spotlight shows that millennials (ages 20-39) are twice as likely to report losing money to online shopping fraud than their older counterparts. Online shopping fraud reports include complaints about items that are never delivered or are not as they were advertised.

The current pandemic situation has forced almost everyone to adopt digital payments and it has become an essential part of every citizen's life. The rapid rise in cybercrimes can be attributed to this sudden accelerated growth of digital payment adoption by otherwise non-users. For criminals, cybercrime is lucrative, hard to detect and provides ability to target a wider group of users across multiple markets. According to the World Economic Forum, burgeoning cybercrimes can be attributed to - heightened dependency on digital infrastructure (e.g. e-commerce activities, bill payments, communicating over emails, social media, and other digital channels), exploitation of fear and uncertainty by cybercriminals, and increase in time spent online that leads to risky behaviour. Moreover, ransomware attacks have continued to rise as well. According to a recent study done by YouGov and ACI Worldwide, 47% of respondents from Tier-I cities of India are concerned about digital payment frauds.

2.3 Components of online retail transactions

To understand the threats and risks to online retail transactions we must understand the components and methods of the online transactions.

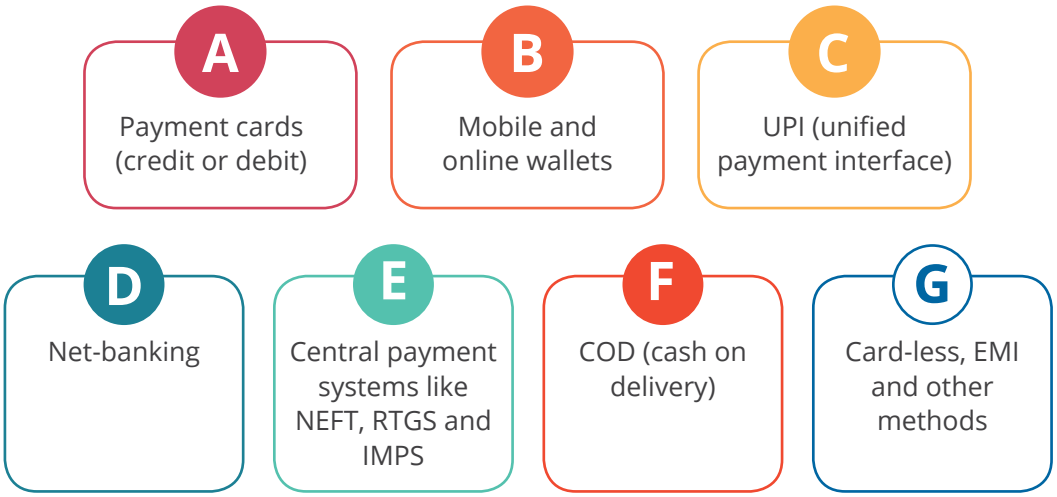


[12]Millennials and fraud: What's the story; Federal Trade Commission - Consumer Information; October 2019

- **Buyer/seller** – individual or corporate
- **Channel** – web, mobile, SMS, IVR, USSD, social media like electronic channels
- **Network** – public or private inter/intranet
- **Systems** – Payment gateways, Banks, mobile money, switches, ATMs, aggregators, databases, search engines, websites
- **Product/Service** – physical or virtual products or services

There can be more than one such entity involved in one e-commerce transaction on each direct buy or sell. From the above illustration of typical actors involved in e-commerce transactions, each and every entity and interface point are a potential threat to become part of fraud in the overall transaction process.

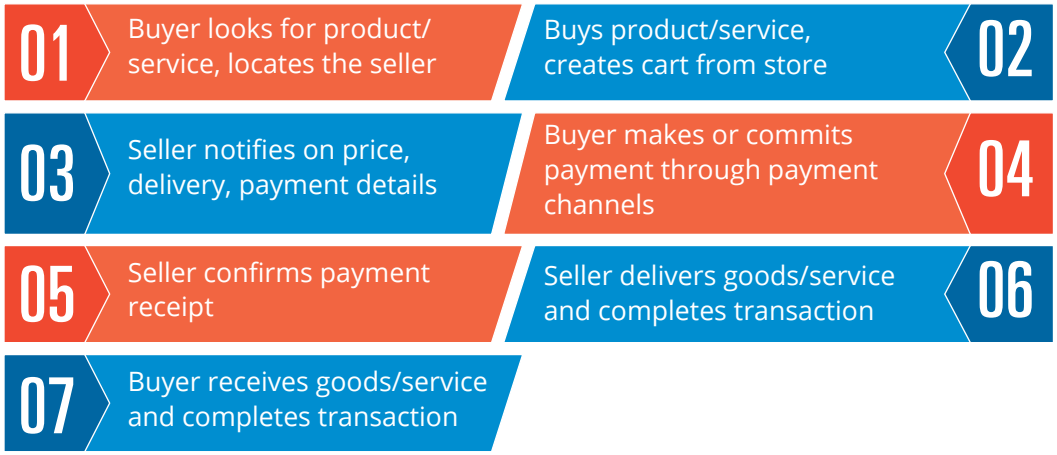
Merchants offer several methods for payment:



Merchants design and host web-based portals as a marketplace with an inventory of products or services. The marketplace could also be an application on the mobile. Merchant ties up with a payment gateway which processes these payment methods and links the merchant with his bank.

Consumers use these portals or apps to view products and place an order on their portal or app. Merchant redirects the consumer's order to payment gateway, which authenticates the confidential payment information provided by consumer. Payment gateway passes on the information to bank which confirms or rejects the order based on several parameters like balance or password.

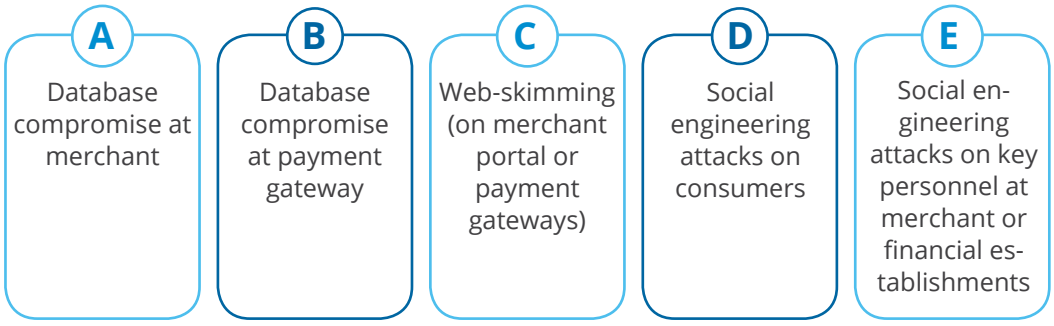
2.3.1 E-commerce transaction cycle- Seller & Buyer:

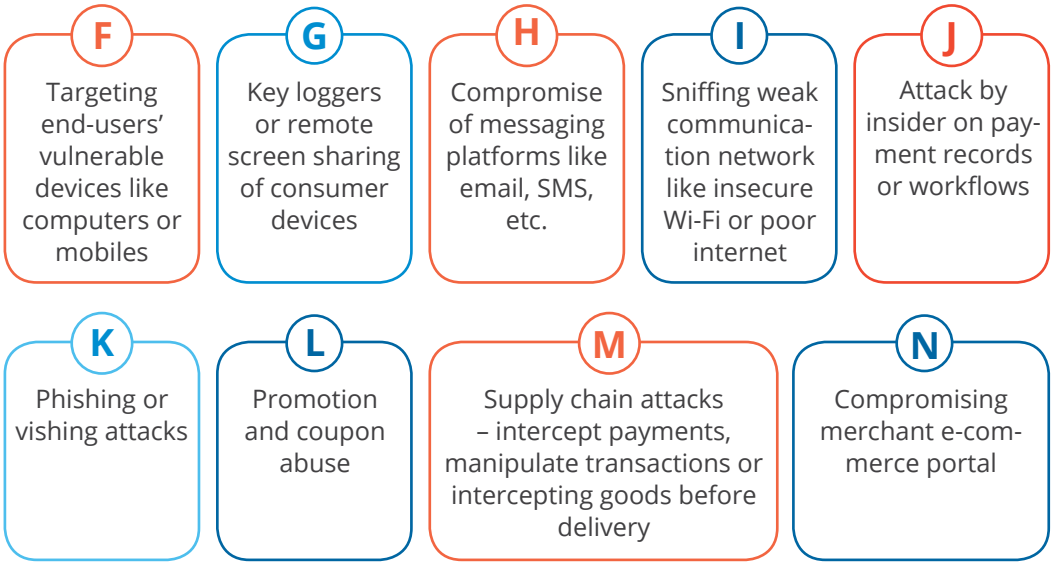


It is clear from the above description that online transaction channel introduces exposure points at various points of the cycle. Below chart summarizes just how different entities in the transaction cycle are vulnerable.

Vulnerable entity	How are these vulnerable
Merchant process	Not following PCI DSS compliance increases the risk of debit and credit card information loss
IT infrastructure	Servers, databases, network, etc. impacting merchants, aggregators, consumers performing transaction through affected infrastructure
Payment gateway	Lack of implementation of fraud management tools and encryption
Consumers	Vulnerable with social engineering or technical attacks can target one or more consumers
Business process	Vulnerable business processes with weak or missing control affects one or more stakeholder(s)

Some attack methods or threats used to execute frauds:





To execute a fraud, the criminal can use any of the entry points as mentioned in the list of entities involved above. Established and regulated entities like banks or processors are normally difficult to compromise and are less targeted.

2.4 Modus operandi of recent fraud cases

Here are some well-known data breaches that impacted the online retail industry in India. The modus operandi of these breach and attack methods are also discussed.

A ORGANISATION LEVEL

In 2017, an anonymous user claimed on forum that he has hacked this firm's database and 17 million records including usernames and passwords are on sale. The company acknowledged the leak and responded with resetting passwords for all its users and public assurance of improving security in its product. The passwords were said to be hashed with salt and hence not easily recoverable.

Similar data breach was experienced with a large music streaming service with over a million account details including email, passwords, social profiles, date of birth was made available online. The passwords were hashed using a weak algorithm MD5 which made it easy to reverse.

Another similar data breach with an online travel agency was made which involved 18 million user records being made public.

The modus operandi in the above cases generally are compromise of weak login credentials in the infrastructure which manages live user data. These are relatively easy for a criminal to compromise. The systems and applications are exploited with dictionary or brute force attack till the right password or credentials are obtained. The attackers generally will have large database of weak passwords.

On the other hand, the impact of such breaches occur to users when they use the same passwords for other services like email, social networking sites, etc. These weak hashes from database dump can be used to recover the original passwords

which then can be used to compromise users' other accounts like email, social media or steal their identity. Identity theft can work at both levels – end consumers as well as merchants. Cybercriminals can set up fake merchant accounts on behalf of legitimate businesses and redirect the payments. Similarly, once criminals obtain partial information, this can be used to create a fake identity and extract remaining information via email, phone or any other social media tactic.

B ORGANISATIONAL LEVEL

Web Skimming

A recent attack where the webpage of a large international airline was hacked; users booking tickets were redirected to an unauthorized server and their payment card information were collected. This breach was active for several months before being discovered, with half a million records stolen. This kind of attack is like ATM skimming where hardware devices are mounted on the ATM card reader.

Here the modus operandi is an elaborate act of compromising the web server where online flight booking and card transactions are done. Card details of consumers are captured and sent to an illegal server.

C PAYMENT PROCESSOR LEVEL

Fraudulent collect requests in UPI and online wallets

Mobile wallets are ubiquitous and used by millions of users. As per India Digital Payments Report 2020, the number of transactions done in Q1 2020 was 1.08 billion[13] and the value of transactions was INR 429 bn in India. Mobile wallets help people do peer-to-peer (P2P) and consumer-to-business instant money transfer with much ease and convenience. Money can be sent to a mobile number or VPA (virtual payment address) linked to their bank account or an online wallet. Similarly request for money can be sent via a collect request to a user. This feature has been misused by many fraudsters to send collect request to unsuspecting users instead of sending money. Users accept and enter their PIN or password without verifying the requests and lose money. Though there are caps on maximum transfer amount, fraudsters play under the limits & trick people. In some cases, fraudsters contact the user over phone or other channel and convince them using social engineering methods to accept the request.

The modus operandi here lies in abusing user attentiveness and app's mediocre user interface. Though executing this fraud largely depends on the users' lack of alertness, it also makes uses of complex functionality of apps and risks associated with such new methods. In some cases, this is compounded by similar looking send and collect requests alerts or app interface. This comes down to poor design and UI/UX (user interface/user experience) issues. Many apps don't clearly distinguish using different menu, colours, icons or alerts to help users understand and differentiate between requests.

[13]Mobile wallets Q1 transactions volume drops 4% in India; Economic Times; May 2020

D MERCHANT LEVEL

Fake marketplace or seller

There have been few cases where fake e-commerce marketplaces or customer support numbers have been setup to lure people into fraudulent business. These sites or contact details appear in web search results, accept orders from people and then dupe them. Fake customer care numbers gather sensitive financial details or passwords and dupe the customers. Several cases of fake sellers also appear in genuine online retail marketplaces and defraud customers with fake or non-existing products.

Even merchants or sellers also have been defrauded by criminals by falsely claiming failed delivery of products.

The modus operandi here is to abuse a social platform or a trusted marketplace to sell fake products. In some of these platforms, the sellers are not sufficiently verified for their authenticity.

E CONSUMER LEVEL

Phishing

Phishing is one of the simplest and quickest fraud methods employed by criminals. Everyday hundreds of people receive phishing calls, emails or messages luring them to visit a website or link and share sensitive banking or personal information. They use social engineering methods to lure people in divulging banking or e-commerce account details. In phishing, criminals have risked taking longer time or repeat calls or messages to obtain sensitive details or initiate online fund transfers from unsuspecting users.

The modus operandi in phishing is plain and simple social engineering. Criminals send genuine looking email or message to unsuspecting users to lure them into the fraud.

F CONSUMER LEVEL

Identity Theft

Identity theft is another common and age-old method of online fraud. The modus operandi here is that criminals get hold of users' information to reset the account password or e-commerce portal. They also obtain users' login credentials by way of social engineering, database breach or other illegal means. If they are able to compromise a user's email account, then this can be used to reset or change password of online banking and many other services.

G BUYER SIDE FRAUD

Frauds can also happen at the buyer side as well. The modus operandi adopted by the fraudster is to file fraudulent claims, chargebacks or use compromised payment cards. Fictitious consumer accounts are created with the intention of making purchases online using stolen financial information. The return policy guarantee, provided by the online marketplace is also abused by the fraudsters.

A criminal case[14] was registered in Rajasthan against an engineering graduate and a student for allegedly duping an e-commerce company to the tune of INR 1.05 cr and 152 very expensive mobile phones by falsely claiming that they were delivered with empty boxes in place of phones. The fraudsters had been ordering expensive mobile sets with different names, IDs and addresses. Then, they used to get refund from the company by falsely claiming that they have received empty boxes.

H BUYER SIDE FRAUD

Cyberabad Police in India investigated a criminal case[15] in which a man and his family members would first place orders of expensive items from the online shopping websites using fake credentials. Later, when the shipment gets delivered, they would remove the items from the boxes and replace with duplicated items, accusing the sellers of sending sub-standard items. The online marketplace companies used to replace the products or refund the fraudsters.

I FAKE UPI-BASED PAYMENT LINK

In this case, the fraudster asked the victim, a Pune-based trader, to transfer a nominal amount of INR 10 to a mobile number from his digital wallet[16]. It was presented as 'registration fee' to initiate the online purchase of a scooter. Subsequently, he received payment links where he had to enter his UPI ID and OTP received and send it back to the fraudster. The information was used to transfer INR 1.53 lakh out of his accounts.

In another case, a Pune resident who wished to sell his air-cooler was tricked by a prospective buyer who agreed to pay INR 9,000 through a UPI-based app. However, the latter sent a 'pay' request to the former, who promptly authorised it without realising that the amount would be debited from, not credited to, his account.

J REMOTE ACCESS MOBILE APPLICATION FRAUD

Fraudsters, had listed fake numbers online under an NGO's name, gained access to a Mumbai resident's debit card details by asking the victim to download Anydesk, a remote desktop software tool, which provides a third party complete view of the user's screen. The fraudsters tricked the victim to share the card details and INR 30,000 was siphoned off from it.

[14]Flipkart 'duped' of Rs1.05 crore, 152 smartphones; two youths arrested; Livemint

[15]Man who cheated e-tailers Flipkart, Amazon of Rs 36 lakh arrested; Hindustan Times

[16]8 digital payment-related scams and how you can avoid them; The Economic Times; December 2019

03

MINIMIZING RISK IN ONLINE DIGITAL PAYMENTS

Minimizing Risk in Online Digital Payments

> As of March 31, 2019, 925 million debit and 47 million credit cards have been issued in India. In respect of debit cards, India is second only to China[17].

3.1 The present situation

At the end of 2012, India had 331.60 million and 19.55 million debit and credit cards respectively which grew to 861.70 million and 37.49 million cards respectively by the end of 2017. By March 2019, it grew to 925 million and 47 million debit and credit cards respectively.

India is one of the few countries which has fast payment systems in the form of IMPS and UPI. IMPS which was introduced in 2010 is a robust & real-time fund transfer service which offers an instant, 24x7, interbank electronic fund transfer service that could be accessed on multiple channels like Mobile, Internet, ATM, SMS, Branch and USSD.

Similarly, UPI provides an additional convenience to customers who do not wish to provide their card numbers, IFSC codes or account numbers for performing transactions. Fraud methods like phishing, identity theft and collect request frauds are generally successful because consumers lack knowledge or alertness during the attempt. The rapid growth of mobile, internet and payment industry has enabled these advanced payment and e-commerce products to be used by consumers. Consumers have rapidly adopted these digital channels, however with low awareness of safety. Such products and payment instruments coupled with new age gadgets, web apps and concepts make them susceptible to frauds.

3.2 Actions taken by Government

Government of India has launched the portal *http://www.consumerhelpline.gov.in* to provide a platform to consumers to register their complaints. Further, the National Consumer Helpline (NCH) has partnered with some companies to resolve their customer complaints. This is an alternate grievance redressal method and is a completely voluntary initiative taken up by these companies. 5,620 cases related to fraudulent online shopping cases were registered in Q1 & Q2 of 2019 against 4,955 cases registered in the financial year 2018-19[18].

[17]Benchmarking India's Payment Systems; RBI Report; June 2019
[18]Ministry of Commerce & Industry Department for Promotion of Industry and Internal Trade, Lok Sabha Unstarred Question No. 3824.; December 2019

The Reserve Bank of India has taken cognizance of the imperatives of enhancing the safety and security of online payment systems and has taken necessary steps related to security and risk mitigation for securing the payment transactions. Few of them are:

- Vide circular on 'Security and Risk Mitigation Measures for Electronic Payment Transactions' dated 28.02.2013, RBI has directed banks to introduce additional measures to secure electronic mode of payments like RTGS, NEFT and IMPS.
- RBI has issued guidelines on Regulation of Payment Aggregators and Payment Gateways dated 17.03.2020, which attempts to regulate in entirety the activities of Payment Aggregators and also provide baseline technology-related recommendations to Payment Gateways[19].
- Vide 'Master Direction on Issuance and Operation of PPIs' dated 11.10.2017 and updated as on 29.12.2017, PPI issuers were instructed to put in place a framework to address safety and security concerns for risk mitigation and fraud prevention.
- RBI has issued various instructions in respect of customer protection. Vide circular dated 06.07.2017. RBI has issued directions limiting the liability of customers in unauthorized electronic banking transactions.
- Similarly, vide circular dated 04.01.2019, RBI has issued directions limiting the liability of customers in unauthorized electronic payment transactions in PPIs issued by Authorized Non-banks. Vide circular on "Harmonization of Turn Around Time (TAT) and customer compensation for failed transactions using authorized Payment Systems" dated 20.09.2019, the framework for TAT for failed transactions and compensation has been prescribed, and the prescribed TAT is the outer limit for resolution of failed transactions.
- For non-banking entities operating payment systems in India, in order to ensure that the technology deployed to operate the payment system(s) authorised is/ are being operated in a safe, secure, sound and efficient manner, RBI has, vide circulars dated 07.12.2009 and 27.12.2010 (as subsequently amended vide circular dated 15.04.2011), mandated System Audit to be done on an annual basis by a Certified Information Systems Auditor (CISA), registered with Information Systems Audit and Control Association (ISACA) or by a holder of a Diploma in Information System Audit (DISA) qualification of the Institute of Chartered Accountants of India (ICAI).
- For securing card transactions, banks have been advised to provide online alerts for all card transactions {Card Present (CP) and Card Not Present (CNP)}, vide RBI's circular dated 29.03.2011. Vide circulars dated 22.09.2011, 28.02.2013 and 24.06.2013, banks have been advised to introduce additional security measures for securing electronic (online and e-banking) transactions.
- Banks have been directed to mandatorily put in place an Additional Factor of Authentication (AFA) for all CNP transactions w.e.f. 01.05.2013 failing which the issuer bank shall reimburse the loss to customer without demur.

[19]Guidelines on Regulation of Payment Aggregators and Payment Gateways; Reserve Bank of India; 2019-20

All authorised card payment networks are permitted to offer card tokenisation services to any token requestor (i.e., third party app provider), subject to all extant instructions on safety and security of card transactions, including the mandate for AFA/PIN entry, vide circular dated 08.01.2019.

3.3 Safety of the consumers and other players in the ecosystem

The success rate of frauds are high when they're executed through electronic channels like email, SMS, phone, social networks, etc, since people generally can't read or sense threats from criminals communicating electronically. Culturally, the risks and threats of a traditional business are ingrained in people and they can reasonably protect themselves against such frauds. But they lack experience when it comes to electronic or modern ways of business.

- More nuanced education on payment tools, infrastructure, and contemporary concepts on payment cards, wallets, online or mobile based transactions must be done.
- Sensitization of risks and threats of modern tools and apps must be made to consumers just as done for a traditional method like banks, cheque books and signatures.
- Do not burden the consumer with different authentication credentials or multiple instances of PIN, password, OTP, and biometric passwords. Unification and standardization of these into just one or two methods are much needed in the industry.
- The products apps and tools must have clear and concise interface and experience when it comes to payment processing or handling finance of the consumers.
    - The interface with message or activity must be explicit, not ambiguous and should aid the consumer in taking his or her decision.
    - The authentication must happen just before the transaction is being processed and not at an early stage of activity.

3.4 Compliance with the laws

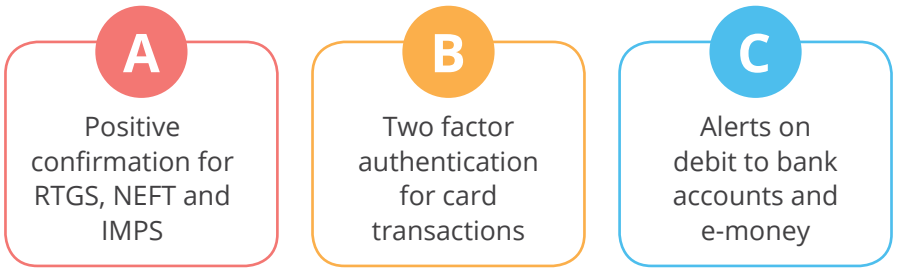
Owing to the cross-cutting nature of e-commerce, different laws and regulations across sectors govern the present e-commerce activities, some of which are:

- Income Tax Act, 1961
- Consumer Protection Act, 1986
- Information Technology Act, 2000
- Foreign Exchange Management Act, 2000
- Payment and Settlement Systems Act 2007
- Companies Act, 2013 and
- Laws related to Goods and Services Tax

The payment systems in India are built keeping efficiency, consumer safety and security as prime importance. The payment and settlement systems are adequately regulated and supervised by the Reserve Bank of India. We are witnessing a number of innovations taking place in the digital payment industry which are reshaping the payment processes.

The ecosystem of online retail industry involves several players like marketplace, merchants, payment gateways, financial institutes like acquirers and banks and card networks. The government, certification and industry agencies and regulatory bodies play the overseeing and governance aspect. The central bank has regulations on how banks (or issuers) handling transactions should have controls in place for detection and prevention of frauds, and continuous monitoring. Industry agencies like PCI has standards on securing systems for merchants, marketplace, payment gateways and device manufacturers. Regulatory bodies like NPCI (and PCI also) has standards for payment processors.

The Reserve Bank of India has a framework for limiting the liability of customers in cases of unauthorised electronic banking transactions. RBI has also introduced the following mandatory guidelines:



The Ombudsman scheme for Digital transactions was launched in order to facilitate the redressal of complaints regarding the digital transactions undertaken by customers of a Payment System Participant viz., any person other than a bank participating in a payment systems (banks are covered under the Banking Ombudsman Scheme).

Companies who develop apps, wallets and tools for consumer use, only have a few compliance requirements to meet. PCI DSS and information security standard ISO 27001 are industry requirements and not mandatory government or central bank requirements. The central bank regularly publishes guidelines to be followed for entities operating in this ecosystem to help curb frauds in retail industry. In addition to the regulatory compliance, regular internal and external audits must be performed to make sure the systems are safe and secure.

Strengthening the laws and procedures especially dealing with cross-border transactions would help the enforcement agencies to detect and prosecute fraudsters who target the consumers by exploiting the gaps present in investigation procedures. When a data breach happens, the entity should be equipped with minimum requirements to handle the incident effectively till formal investigation begins. This would ensure that there is no loss of critical evidence attributing to the attack and attacker with private or government organization, the entity has no obligation to inform consumers or government on the incident or breach. Currently public breach notifications are not mandatory in India.

More recently, the Personal Data Protection Bill, currently under review with the Joint Parliamentary Committee seeks to establish a strong and robust Data Protection framework for India, and a Data Protection Authority for regulating the privacy of Personal Data and empowering the citizens with rights related to their personal data.

Further, on issues relating to non-personal data, Ministry of Electronics & Information Technology, Government of India has constituted a committee of experts to deliberate on the Data Governance Framework.

The Government of India with a vision of putting in place an institutional framework covering various areas of e-commerce, prepared a draft national e-commerce policy and placed it for comments in the public domain. Views/suggestions from different stakeholders including several e-commerce firms on the various provision of the draft have been received. At the time of writing this report, the views/suggestions thus received are still under consideration by the ministry.

Section 79 of the Information Technology Act, 2000 elaborates on the exemption from liabilities of intermediaries in certain cases. Section 79(2)(c) mentions that intermediaries must observe due diligence while discharging their duties, and also observe such other guidelines as prescribed by the Central Government. Accordingly, the Information Technology (Intermediaries Guidelines) Rules, 2011 were notified in April 2011.

The Ministry of Electronics and Information Technology is in the process of amending the Information Technology (Intermediary Guidelines) Rules, 2011. Comments & suggestions from all the relevant stakeholders were sought in this regard.

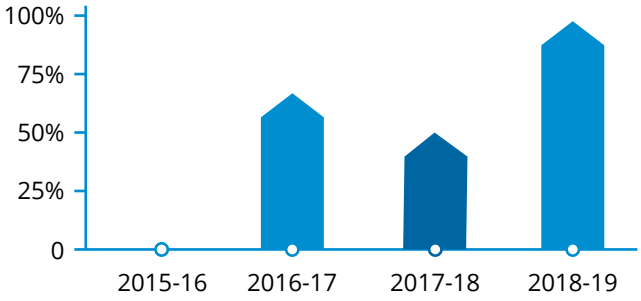
> We have seen fraudsters becoming more and more sophisticated in finding innovative ways to cheat the consumers through e-commerce and banking transactions. Criminal syndicates across the globe are deeply involved in stealing of customer information and misuse them. Prevention is always a better option; we need to educate the consumers to protect themselves from the fraudsters. Awareness among the consumers and implementation of fraud risk management by the businesses is one very important step in that direction.
>
> **Harikishore Kusumakar IPS**, IGP, West Bengal Police

3.5 Promoting adoption of Digital payment

Apart from mobile and internet penetration, the Digital India campaign by Government of India has largely influenced the increased adoption of online payment and e-commerce transactions. Government of India withdrew the legal tender status of INR 500 and INR 1000 notes in November 2016 with the objective to eliminate black money and to curb the infusion and circulation of fake Indian currency notes. There have been multiple reports, however, that there is a steady infusion of fake currency to support illegal activities in the country.

The Special Investigation Team (SIT)'s fifth report, mentions that large amount of unaccounted wealth is stored and used in the form of cash and also there have been huge cash recoveries by law-enforcement agencies, from time to time[20]. This has resulted in a push for using cashless payment systems including cheques and digital payments. Regulatory body like NPCI, the central bank, and several industry bodies have also pushed organizations to adopt digital payments.

Adoption of E-Payments in India



ATM	Volume (mn)	Value (INR bn)	Ticket Size (INR)	Share (Volume)	Share (Value)
Credit Cards	9.77	45.33	4639.19	0.10%	0.14%
Debit Cards	9859.61	33107.89	3357.93	99.90%	99.86%
PoS & Online	**Volume (mn)**	**Value (INR bn)**	**Ticket Size (INR)**	**Share (Volume)**	**Share (Value)**
Credit Cards	1762.59	6033.48	3423.08	28.54%	50.41%
Debit Cards	4414.28	5934.59	1344.44	71.46%	49.59%

[20]https://pib.gov.in/newsite/mbErel.aspx?relid=158183

The rapid increase of mobile phones and its usage as personal devices to make online payment has ensured that banking transactions reach everywhere. Also, there is a significant rise in the number of non-banking entities in retail payment space. The companies that provide online payment services innovate and adopt newer technologies that allow NBFCs, mostly fintech companies to compete in areas not yet dominated by traditional banks. There is a steep increase in the usage of e-money, UPI, Aadhaar Payments Bridge System, RuPay, Bharat Bill Payment System, etc.

In addition, government and industry must also help organizations understand the security risks and threats of digital transactions and payments. Businesses must be advised on minimum controls to protect data privacy and security of consumers before offering services to them. Appropriate awareness and training campaigns must be carried out regularly to government departments and businesses on novel fraud methods and ways to protect from them.

Government must also train, equip and strengthen prosecution and law enforcement agencies on handling and punishing culprits in cybercrime cases. Government and regulatory bodies must be equipped to take Suo Moto action on entities that had large scale breaches impacting public at large.

3.6 Impact on government revenues/taxes/economy

There are both tangible and in-tangible impact of frauds in online payment space on government. The stability of the country's economy becomes affected if the financial structure is afflicted with frauds. The frequency, complexity and the inherent costs of online frauds have caused the regulators to take necessary steps to avoid any impact on the Indian economy.

Non-tangible impact

- Like any other negative aspect, e-commerce frauds impact Government morale, citizen confidence, external perception, social security impact, and its ripple effect to the economy, investments, mandate to introduce hurdle on business.
- Panic among citizens about the safety and security of the payment system especially when misinformation spreads in no time.

Tangible impact

- Increase in legal overheads, revenue and tax impact, immediate and ripple effect on economy, and thereby negatively impacting the society.
- Any attempt to over-regulate the stakeholders involved in the online payment space may be detrimental.
- Delays in the legal procedures related to reporting, investigation and prosecution due to growing number of fraud cases.
- Profitability of the institutions from online retail space would decline which poses threat to the economy.

To serve the growing needs of the Indian economy, we need a safe and efficient payment system that can counter the newer methods adopted by fraudsters.

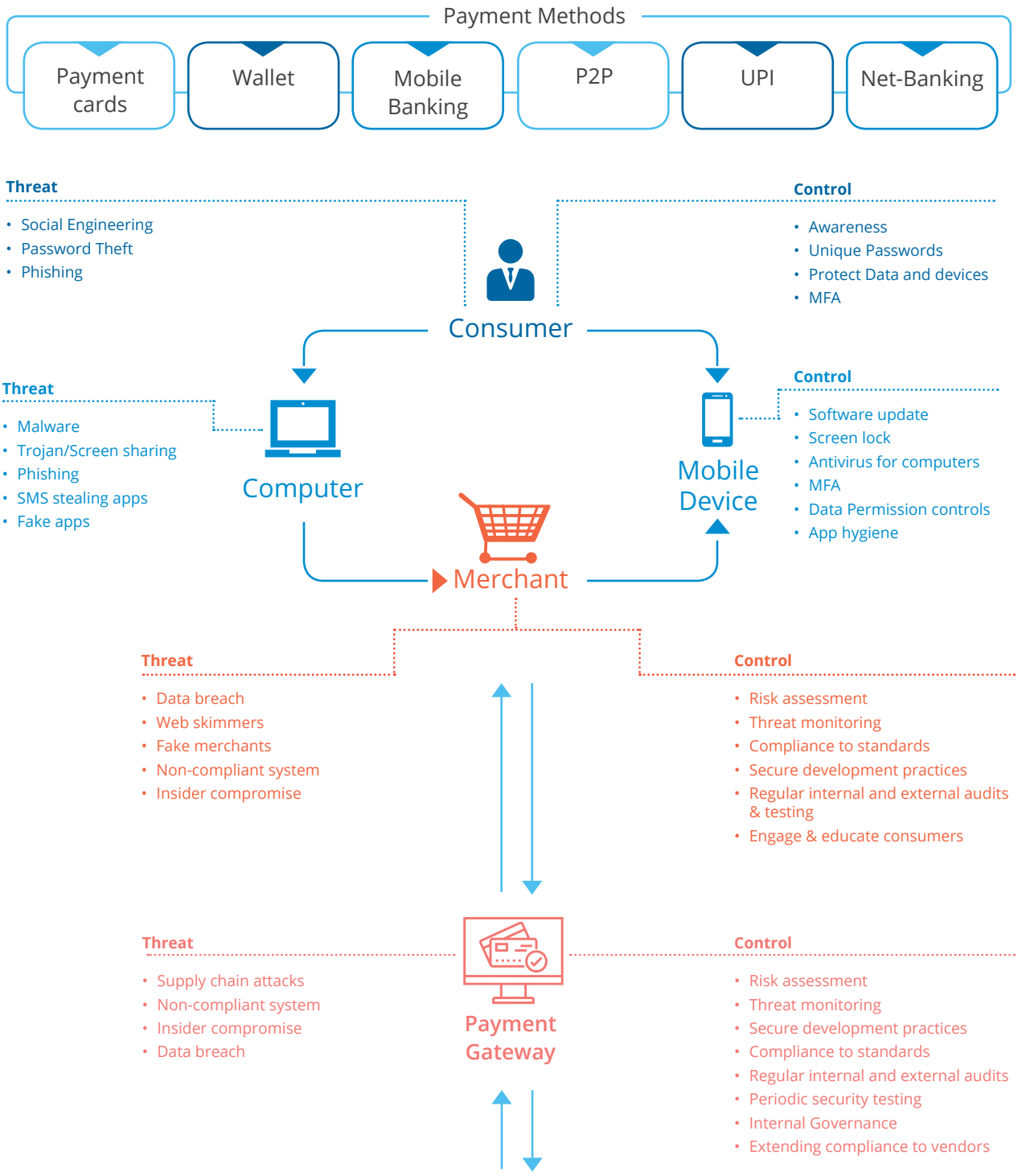
04

COMPONENTS OF PAYMENT TRANSACTIONS FROM THE PERSPECTIVES OF FRAUD AND RISK

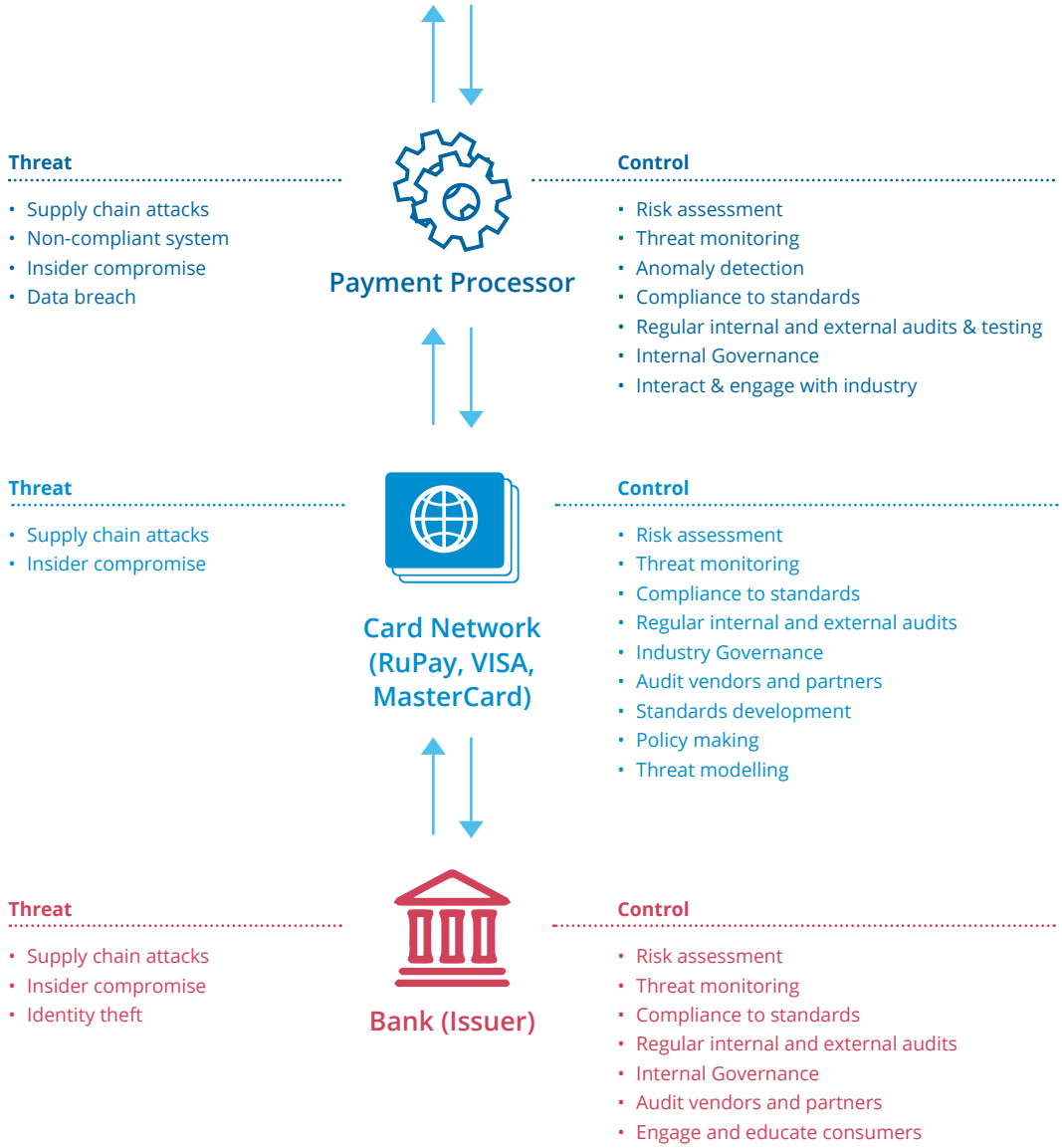
The ecosystem of online retail industry & payment transaction involves several components such as players like marketplace, merchants, payment gateways, financial institutes like acquirers, banks and card networks, architecture, interfaces, processes, devices and actors, apart from the consumers.

The below figure shows typical threats associated with online payment transactions.

Payment Transaction Flow and Threat Scenario



Payment transaction flow and threat scenario contd...



Government, Regulatory and Industry Body

Control

- National policy and framework to protect nation assets and citizens
- Standards development
- Support businesses, industry and merchants
- Improve laws and legal ecosystem to protect consumers and businesses
- Audit vendors, partners, processors and issuers
- Empower and upskill prosecution and law enforcement
- Empower industry for Innovation and continuous development
- Engage with global partners
- Skill and threat information exchange with internal and external entities


IDEA
seo
4000 4589 7568 1547
JANE WALKER

05
CATEGORIES & TYPES OF FRAUD

Categories & types of Fraud

E-commerce frauds are broadly categorised into:

BUYER SIDE FRAUDS
Fraudulent claims, chargebacks, fake buyer accounts, promotion or coupon abuse

MERCHANT SIDE FRAUDS
Selling counterfeit, non-fulfilment

CYBER SECURITY FRAUDS
Account takeover, identity theft, card details theft, etc.

Below listed are typical well known types of fraud but it is not an exhaustive list.

5.1 Card Not Present (CNP) Fraud

The fraudster makes use of stolen card information without presenting the actual card itself. Using someone else's financial information, the fraudster makes purchase at an online store. The acquirer bank checks the card information and approves the purchase, the goods are then delivered. The original cardholder asks for chargeback and the online store makes the reimbursement and is left with a loss.

5.2 Clean Fraud

When a fraudulent transaction with all the checks appears to be valid, like customer identification, account details, endpoint identifier, location, IP address, billing address, card, 2D authentication vector. This means that a fraudster is able to access or steal every detail required by the genuine customer. These are difficult to detect with generalised controls. One way to combat is by mixing service transaction legs with different authentication mechanisms every time and introducing on the fly interaction with the user. However, this can introduce hurdle to customer experience.

5.3 Account takeover Fraud

Where fraudster gains access to customer account and adds or updates or replaces some of the information with their own information. For example, delivery address, email id, mobile number in the customer profile. In these frauds, customer would be able to detect only after the transaction completes.

5.4 Friendly (Chargeback) Fraud

In this case, merchant receives a chargeback because the account owner (customer) denies making the purchase or collecting the order but the product/service delivery is actually completed. This type of fraud is generally lined with re-shipping in some cases. These type of frauds are called 'friendly' since the order might have been placed by a friend (or relative) who has access to customer account details.

5.5 Identity Fraud

Fraudster acquires or uses sensitive personal information like passport, Aadhaar, driving license, etc. and uses this information to create mirror user identity to perform multiple frauds.

5.6 Affiliate Fraud

Fraudster aims to gain from an affiliate program by manipulating transactions or registrations. For example, an increasing number of registrations with fake accounts using automated tool. This is also tagged as promotion or coupon abuse. According to our analysis, promotion or coupon abuse is rampant in India where end customers create multiple fake/synthetic accounts. This is also an extension of signup fraud as there is a good amount of money new start-ups and established companies write-off each year. To counter fraud, validation against third party data can be used to fight against this fraud. Apart from all the analysis using merchant's own data, there is a value in cross referencing identities across multiple lists, repositories and consortiums.

Referral payout abuse and cart abandonment abuse are also commonly observed abuse and are an extension of Affiliate Fraud type. Referral program is a great incentive to create fake accounts or posting referral codes on social media. If the customer abandons his cart for a longer duration, discount is offered to such customer as a sales strategy.

There are number of steps that can be taken in order to fight the abuse. Some examples are:

- Implement process tracking
- Limitation on rate and duration of validity of promo code
- Implementing customer identification parameters
- Geo-location tracking
- Limited disclosure on coupons
- Controlled distribution of coupons

5.7 Triangulation Fraud

The fraud is carried out via three different points:

A Fake online store offering low prices, and collect address and account details as a purpose

B Using original account details collected to order goods at real store to ship to original customer

C Stolen account details to make additional purchases

Such combined methods to perpetuate fraud like b and c, it is hard to detect fraud and it results in greater damages to both merchants and real users.

5.8 Merchant Fraud

A method used where goods or services are offered at very cheap prices but either counterfeit products are shipped or actual good/service is never shipped. In these cases, no-chargeback payment methods are used. Customer will not have access to the helpdesk to raise concern. This is applicable for both retail and wholesale transactions.

5.9 Miniature Fraud

Repeat fraud with small amount in the name of charges, service tax, etc.

5.10 Pharming

Fraudsters set up mirror or illegal sites that look like genuine ones, misdirecting customers to fraudulent sites without their consent to collect payment information, at the time of purchase, and use the information to perform other frauds.

5.11 Botnet

Fraudsters infect network or machine to stole identity or account information. When a transaction is initiated from an affected machine or network, the fraudster captures required information without the knowledge of the merchant or customer. This fraud could result in high magnitude frauds, as the fraudster can only sell the stolen information and might not use it directly to perform fraudulent transactions.

5.12 Phishing / Whaling

An act of sending communication by email, SMS, voice call or any other means to steal sensitive information like personal details, account, identity, passwords, card numbers, PIN, OTP, etc.

Whaling is also a similar act of phishing that targets specific type of consumers, like business heads. E.g., Fraudsters send information to business heads pretending business partner or regulatory body to collect payment, company information or account details.

> It is a well established fact that the basic line of defence against any fraud is internal controls in the businesses. Technology has the ability to reduce the chances of human connivance and can be used to make the fraud prevention and detection more effective.

M D Sharath, Superintendent of Police, Cyber Crime Division, Karnataka

> The number of successful attempts in defrauding the online retail merchants is growing rapidly due to increasingly sophisticated attack tactics used by the fraudsters. We have seen consumers aren't even aware that their card information is stolen and used for fraudulent purchases till they receive their bill. It is a tricky situation for the businesses to adopt adequate fraud prevention measures that are secure yet doesn't affect the user experience.

Raghavendra K. Hegde, Superintendent of Police, Financial Intelligence Unit, Karnataka

06

FUTURE FRAUD POSSIBILITIES

Future Fraud Possibilities

Below are some of futuristic fraud scenario possibilities, briefly mentioned:

Spoofing fraud prevention control parameters – location information, endpoint identifiers, goods/services identities like SKUs/Barcodes

The current fraud prevention and detection mechanisms are relying on the control parameters like location information, endpoint identifiers, goods/services identities like SKUs/Barcodes. If these parameters e.g., geo-location, device identifiers like IMEI, MAC address etc., are spoofed, then fraud prevention and detection may be ineffective.

Exploiting supply chain vulnerabilities where man & machine exchange is involved

E-commerce is becoming more and more complex with large network of seller, merchant, aggregator, warehouse, delivery mechanisms spread across various levels. This would result in complex ecosystem of human to system and system to human. And, one supply chain leg compromised may result in significant damage to the system.

Exploiting risk transfer controls like buyback, insurance settlement to earlier transactions

Unlike e-commerce transactions, risk transfer controls themselves will become like an e-commerce transaction at a totally different timeline. For e.g., mobile phones coming with buyback insurance policies will get activated after one or two years, all existing controls would be focusing on the current transaction. They will be unable to predict the possible future frauds throughout the buyback duration which would be one or two years from the date of purchase.

07

TECHNOLOGICAL INNOVATIONS & CAPABILITIES LEVERAGED BY ANTI-FRAUD TOOLS

Technological Innovations & Capabilities leveraged by anti-fraud tools

A closer look into application of AI/ML in security

> Customers adopt digital banking experiences expecting quicker, faster and better services allowing sharing of personal data with the financial institutions.

While these data help organisations to use them and improve their offerings, it also leaves them exposed to fraudsters who can breach the data, misuse it or sell it to criminals who operate underground economy. Fraudsters use every tool to take the benefit out of exploiting the vulnerabilities existing within the financial institutions.

Customer identity authentication should not be considered limited only at the time of registration or opening of the account; latest technologies must be applied for subsequent interactions of the customer with the online payment systems. The institutions should be equipped to manage the frauds along with the clear understanding of business and technical challenges. The defence mechanisms should be superior and fast learning solutions that would not burden their customers to perform additional steps to ascertain their identity to perform transactions.

Forced registration, tedious form filling, and additional authentication processes may result in customer frustration which leads to hinder their shopping experience to the extent of abandoning. These inefficient measures would end up creating a problem that is costlier than any fraud that occurs. In a research conducted by Salesforce[21], 74% of customers would like to switch brands if they found the purchasing or checkout process too cumbersome.

[21] State of the Connected Customer; Salesforce Research

The fraud prevention strategies should be designed in a way that avoid taking one-size-fits-all approach which will force all customers to overcome the same hurdles to prove their trustworthiness. An innovative approach that would integrate the fraud detection and authentication technologies should be adopted. The fraud management and detection methodology employed should be able to proactively analyse the threats and adapt in realtime with regard to any development in the fraud landscape.

The fraud management with human-generated rule sets has its own limitations. Latest technologies developed to aid businesses, not only to anticipate the needs and behaviour of their customers but also provide adequate protection to them. With the increase in computation power, generation of huge amount of data, solutions can be built to identify and prevent fraud. With Big Data being fed to the system, the learning, predicting, acting can be achieved by using Machine Learning without the need of pre-programmed rule sets. The advancements in technology in the last decade has opened a new opportunity for organisations to leverage Artificial Intelligence which is the simulation of human intelligence processes by machines, especially computer systems. The anomalies in the online payment system can be detected by feeding millions of data points about the ecosystem. Hyper-granular profiles of customers, transactions, devices and other relevant fraud indicators built by machine learning models can be the key to unlocking superior customer experience while balancing fraud and risk.

The benefits of using **machine learning** in general are as follows:

- Ability to perform decision on real time basis
- Capability to identify the subtle patterns or variations
- Processing the information without any bias or error
- Significant reduction in costs

The hidden insights and patterns of fraudsters can be best understood by implementing machine learning with data as an inextricable component of fraud management. Machine learning requires access to huge amounts of data to be able to learn and generalize the knowledge. When applied to fraud management, the following can be achieved:

- Reduce manual review process through fast, iterating machine models
- Ability to adapt to new business lines by extensive usage of the experiential data
- Help to reduce false positives with behaviour analysis
- Augment human decision-making with increased accuracy

To achieve the above objectives, most fraud detection tools that are **AI-based** use the following models:

SUPERVISED	UNSUPERVISED	SEMI-SUPERVISED
It relies on training algorithms that use large data sets with known results.	This model attempts to identify the inherent similarities and cluster data in groups. This model may result in transactions with anomalous attributes being grouped together.	A mixture of correctly labelled and unlabelled data is being fed to train the algorithms.

Several algorithms exist which power Machine Learning. The selection of the best algorithm depends on the type of problem, size and available resources. Random Forest, Deep Learning, Support Vector Machines, Neural networks and K-Nearest neighbours are few examples. The scenarios where these algorithms can be used are:

01 Opening of account-enrol only right customer

02 Scoring of customer transaction-identify the risks of fraudulent online transactions. For instance, a user is declined since there were recent transactions in different distant locations.

03 Preventing identity theft-Keep watch on hacking activity by monitoring the user accounts

Some of the important processes to deal with the fraudsters are:

Device Identification

Device Identification is a technique used to establish a "fingerprint" of a user computer or other web access device in order to track their activity and determine linkages between other devices.

IP Geolocation

Geolocation services provide detailed information about a consumer's worldwide location, line speed, domain, etc. It is used primarily to verify the consumer's data to determine where the consumer is at the time of purchase. Geolocation Services can be used for fraud prevention and also be used for export and regulatory compliance.

Rules Engines

The rules engine is a middleware application that allows the creation and prioritization of rules to be used in managing fraud. These engines allow merchants to create rules that can be evaluated on orders as they come in. The rules engine can have many different names, such as "decisioning software," "management software" or "order management."

Proxy IP address detection

Proxy Detection web services allow instant detection of anonymous IP addresses. While the use of a proxy is not a direct indicator of fraudulent behaviour, it can be a useful indicator when combined with other data elements to determine if an individual is attempting to hide their true identity.

CASE STUDY

Detecting fraudulent merchants using Referrer Domain Attributes[22]

Target: Payment processor, who could unwittingly be processing a fraudulent or illegal payment

Fraudster: Unauthorized merchant selling illegal or restricted goods

Modus Operandi: The fraudster is masquerading as a legitimate or approved trader in order to continue to run an illegal or restricted online business, duping the payment processor into accepting its business

Method of Fraud detection: One of the attributes that the Digital Identity Network collects during an online transaction is the referrer domain, which gives the Risk Solution implemented payment processor, the visibility into the webpage a transacting user has visited before hitting the host web page. In this case, the referrer domain attribute shows the payment processor which merchant site the customer is buying from, before they make a payment.

While the machine learning models offer considerable reduction on operation costs and also change the way how the frauds handling teams operate, it is important to note that the adoption of such new technologies should be evidence based and implemented in phased manner. Machine learning models without rules cannot be seen as complete replacement of existing fraud detection strategies.

Challenges in implementing Machine Learning:

While machine learning has a bigger role to play in online retail fraud detection, the online retailers must invest significantly in making real-time decisions leveraging

[22]LexisNexis Risk Solutions-Cybercrime Report; June 2019

hundreds of data points and contextual attributes about every transaction. With the online volume constantly growing, and fraud attack vectors evolving, using only a static rule-based approach is neither effective, nor scalable.

Most vendors offer case studies demonstrating the efficacy of their solutions. However, beyond vendor marketing material, it is challenging to find objective evidence regarding the uplift in fraud detection or reduction in false positives achieved by machine learning as part of a retailer fraud management strategy.

Gartner in its research report[23] strongly recommends that security and risk management (SRM) leaders avoid setting arbitrary internal objectives to move 100% to machine-learning-based decision making without rules.

Most vendors deploy an opaque mix of machine learning models. Without understanding how the solutions work in detail, it is challenging for Security & Risk Management leaders to assess whether they are a suitable fit for their business requirements.

The ideal scenario for retailers is to try before they buy, either by integrating with vendors for proof-of-concept (POC) trials or by providing historical data to vendors. This is impractical, and Gartner sees little evidence of this happening. Integrations demand IT resources and roadmap space for the implementation effort, as well as contracts governing the use of the service and data. The retailer must take the vendor through the entire procurement and implementation phases to run the POC.

> The cyber police experience is, all the online retail payment apps are being exploited by cyber fraudsters mainly due to less security protocols or process; apart from customer's ignorance. The investment on Fraud & Risk Management in Online retail space by the companies is very negligible. I suggest, Security should be a continuous process, not an one-time affair.
>
> **Ramamohan,** Superintendent of Police, Cybercrimes, Andhra Pradesh Police

> The online retail market is growing rapidly. Due to the increased internet penetration in rural areas, the common people are also engaged in online shopping. Since the money transactions are being done online, criminals also make use of technology to exploit the human & technological vulnerabilities. It is the need of the hour to create awareness among the users to not reveal their sensitive/financial information to any person or unsecured online platforms.
>
> **E S Bijumon**, Addl. Superintendent of Police, Kerala State

[23]How to Select a Machine Learning Vendor for Fraud Detection in Online Retail; Gartner; March 2019

08

KEY CHALLENGES

Key Challenges

> Fraudsters are more sophisticated than ever. Fraud has evolved from individual rogues to organised criminal networks operating in countries across the world.

8.1 Fraud detection, enforcement, investigation and legislative challenges

Many organisations are facing challenges related to new account fraud and account takeover by the criminals exploiting the technical loopholes, social engineering and employing deceptive means. There is no adequate awareness among the users in using good password practices. Any verification based on captcha or one-time passwords asked frequently, may result in customer frustration and may also discourage them from enrolment, login or transact. The legacy fraud detection and authentication tools are facing higher false-positive while analysing the user behaviour based on geography, devices or connection methods. The end customer may be using multiple devices like smartphones, tablets, desktops, laptops and even anonymous browsing with the proliferation of privacy enabled tools. The normal & acceptable behaviour threshold is clearly understood by the criminals and they craft required techniques to circumvent the detection tools. If the fraud prevention methods employed has impact on the customer experience of easy transactions, then the businesses may suffer negatively impacting events like transactions cancelled by the customer due to offense, frustration or missed deadlines (time in seconds) due to review activities.

It is not an easy task for an organisation to provide a low friction, seamless customer experience and at the same time managing the authentication and risk management. Forcing the customers to pass through multiple tests to prove themselves may result in loss of customers to competitors. Customers believe that convenience is more important than security.

Advanced fraud detection tools that use machine learning typically learn from the datasets provided by the vendors who offer it to the businesses, this may have significant impact on the detection accuracy and also reduce the customer experience till the time it learns and adopt to the new environment. An increase in number of false positives that would turn away the legitimate customers due to error can be equated to as bad as accepting the fraudulent transaction. Implementation of new technologies by the businesses without proof-of-concept or

trial runs makes it very difficult to assess the suitability and efficiency to the needs and requirements.

The theft of customer information by the fraudster is carried out by exploiting the static data verification methods and impersonate the consumers to entice them to supply their sensitive information. The relevant laws in India dealing with data protection are the Information Technology Act, 2000 and the (Indian) Contract Act, 1872. A codified law on the subject of data protection is likely to be introduced in India in the near future.

The Information Technology Act, 2000 deals with the issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data.

Under section 43A of the (Indian) Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances.

The privacy concerns related to customer data being collected by the businesses have led to introduction of new legislations designed to empower consumers to block attempts by online companies to collect their personal data, particularly with respect to behavioural advertising. If the companies are required to disclose the manner in which the collected information is used, it could expose the techniques used to discover risk of fraudulent activity to fraudsters, enabling them to develop workarounds or alternative technologies.

The Government has notified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The Rules only deal with protection of "Sensitive personal data or information of a person", which includes such personal information which consists of information relating to:

- Passwords
- Financial information such as bank account or credit card or debit card or other payment instrument details
- Physical, physiological and mental health condition
- Sexual orientation
- Medical records and history
- Biometric information

The rules provide reasonable security practices and procedures, which the body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handles the information is required to follow while dealing with

"Personal sensitive data or information". In case of any breach, the body corporate or any other person acting on behalf of body corporate, the body corporate may be held liable to pay damages to the person so affected.

Under section 72A of the Information Technology Act, 2000, disclosure of information, unintentionally and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to INR 5,00,000 (approx. USD 8,000).

8.2 Challenges in the payment ecosystem

1 Organised criminals' involvement

E-commerce fraud has evolved from individual to well organised crime operating in many countries across the world. Explosion of social media, user profile information, behaviour data available at multiple disjointed places is helping criminals to acquire information in one channel and use it in other channel bringing unprecedented challenges to the e-commerce vertical. Cross-channel monitoring for any fraudulent intent is complex challenge to technocrats, governments and corporates.

2 Multiple level awareness requirement

In the current market scenario, multi-vendor multi-technology solution adoption in e-commerce needs awareness at multiple levels like management, IT, consumers, LEA. Especially considering the cost and effort involved in bringing awareness across the stakeholders, small and medium sized companies relay on inferior or ineffective mechanisms of awareness, and resulting in increase in risk.

3 Cost overhead to invest by stakeholders

As a fact, 'Security' is measured in terms of 'ROI' where 'Security' investments are related to just 'protecting ROI', which mean security will remain as a cost overhead and not essential investments by stakeholders/CXOs. Industries have started accepting the reality but still it poses significant challenge for CISOs to ensure budgetary acceptance by the management.

As a sample, theoretically 'Blockchain' technology is considered as foremost suitable for fraud prevention, but adoption of the technology needs considerable investment from the organization to replace existing technology. The same is applicable for SIEM, WAF, IDS/IPS technologies.

4 Privacy laws

Due to stricter privacy laws within India and across the word (like GDPR) itself is a challenge for fraud prevention. Example, if e-commerce companies are required to disclose the technique and manner of collected information is used to conformant to privacy laws, this itself could expose the techniques used to discover risk of

the fraudulent activity to fraudsters, and could be used to develop alternative mechanism to acquire the information to perform frauds.

5 Customer experience

Usage of customer verification tools such as knowledge-based verification, captcha or OTPs that are asked frequently result in customer frustration and discourage the customer for an enrolment, login or purchase.

The behaviour of the customers is becoming more and more dynamic with involving multiple geographies, different devices and connection methods that may result in higher false-positive and challenge rates from existing legacy fraud detection tools. Ensuring friction-less/low-friction experience to the customers & yet prevent any fraud is a big challenge.

6 Advanced attacks

The sophistication and innovation in the methods adopted by the fraudsters can easily bypass many of the legacy tools employed for detection of unusual activities. Continuous investments in developing the detection methods demands considerable amount of research, collaboration and money.

7 Cross-industry or expertise collaboration

Considering the complex ecosystem with multiple stakeholders - customer, merchant, issuers, acquirers, processors, service providers, financial institutions, aggregators need to take collaborative approach of talking fraud. Whereas each stakeholder adopting its own approach of containing frauds in isolated ways to secure themselves, results in increasing risk for other stakeholders.

8 Intellectual property rights – like trademarks, designs, brand names

Protecting IP in terms of duplicate, pirated, stolen items, brand name in e-commerce is a challenge. This will become even bigger concern for the aggregators where they will not have access to the OEMs to address and protect IPs.

> Online retail ecosystem attracts everyone irrespective of their age and to explore it has its risks as much as its versatility. Compromise of customer's financial data and the existence of fly-by-night operators are some of the fears which continue to haunt me as an investigator.
>
> **S. Aravind,** Superintendent of Police, Special Division, Tamil Nadu

09

FRAUD DETECTION AND PREVENTION

Fraud Detection and Prevention

> Fraud detection and prevention is not a one-time task. Instead, it is an ongoing process that primarily comprises monitoring, decision making, anomaly detection, case management and learning to feed improvements in detection back into the system.

The safety and reliability of information, assets, accounts and transactions belonging to customers and businesses are ensured by employing an effective fraud detection program. The fraud detection program should perform real-time analysis of activities submitted by human beings or machines. The transactions should be categorised to flag all those which exceed the organisational risk tolerance. Businesses need to implement fraud detection technologies across all channels in the payment ecosystem as criminals will attack the least protected channel.

The online fraud detection products or services are designed to help businesses to detect fraud that can happen over the web, mobile or any other channels. The detection of likelihood of fraudulent transactions is achieved by running background processes that use numerous contextual attributes and data sets including the geographical location data, device details, user behaviour and transactional activities. Comparison of collected contextual event information with the expected behaviour that is developed using advanced analytics or statistical algorithms will define the abnormal behaviour and activities.

Below table depicts the general steps for fraud detection by many organisations and the benefits and challenges.

S.No.	Type	Description	Advantages	Challenges
1	Bot Detection	Used for detecting any automated attacks	Can detect any non-human activity trying to use any stolen credentials for accessing	Cannot detect frauds like account opening fraud, manual account takeover fraud, etc.
2	Device Intelligence	Monitoring the device activity, calculate the velocity and location of device usage	Can be used to profile genuine user devices	Difficult to maintain the blacklists and whitelists on continuous basis
3	User activity monitoring	Used for detecting any anomalies by monitoring the customer account activity like updates, payments, addition of new beneficiary, location etc,	Risky user behaviour can be identified	False positives may affect both users and businesses. Automated attacks cannot be detected.
4	Behavioural biometrics for profiling genuine customers	Used to collect customer interaction data like mouse clicks, swipes on mobile devices and keystrokes.	May be used to learn about the user genuine behaviour and anomalies.	Conventional frauds like social engineering and account opening fraud can't be detected
5	Manual Fraud Review	A team of individuals reviewing each transaction (or a selection of transactions) to detect fraudulent activities	Humans are better in understanding the context than automated tools	Time and resource intensive. Difficult to handle any sudden spike in sales

The main objectives of any good fraud detection solution would be to continuously profile the behaviour of consumers, accounts and transactions. Also, ingesting and integrating the external threat intelligence into fraud detection analysis and operations. The fraud detection solutions provide alerts to help the businesses to take appropriate follow-up action such as:

- Putting on hold the transaction if the consumer behaviour is beyond the boundaries of what's expected
- Help conduct further manual review and investigation of the suspect transaction
- Detecting account takeover, which can occur when user account credentials are stolen, such as via malware-based attacks
- Detecting identity fraud when a fraudster sets up a new account, or conducts an unauthorized transaction using a stolen or fictitious identity
- Detecting the use of a stolen financial account (such as a stolen credit card) when making a purchase or moving money from one account to another

The fraud detection algorithms or engines integrated at the enterprise applications have the capability to assess the fraud risk that can occur during the transaction, user navigation or any changes made in address, payment or sensitive information. In order to identify the unusual transaction behaviour, the fraud detection tool should profile various entities such as users, devices including mobile phones and personal computers.

Fraud detection uses rule-based policies that are based on human judgment and knowledge and/or predictive mathematical models to score the likelihood of fraud for a given transaction.

The severity of transaction risk is ascertained through various methods — for example:

- "Printing" the user access device (if there is one) and comparing it with other attributes of the transaction or groups of transactions
- Analysing user or account behaviour, and comparing it with the user's and account's profiles
- Using peer group analysis, which compares an individual entity or group of individual entities with their peers to spot suspected deviations
- Using entity link analysis, which helps detect criminal rings or linked entities engaged in fraudulent behaviour

Advanced fraud prevention tools should have the below main features[24]:

- **Machine Learning**: Uses real-time insights that are fed into supervised and unsupervised anomaly detection methods to find fraudulent patterns in online transaction information or user behavior patterns. Machine Learning algorithms perform complex calculations at a much faster rate when compared with manual review and can raise alerts.
- **Automated Workflow**: Speeds up workflow by automating payment fraud checks, processing order details, blocking suspicious devices, cancellation of fraudulent orders, etc.
- **Insights Dashboard**: Highlights suspicious activities and presents relevant fraud prevention data in a single interface, without switching between multiple screens, that can effectively execute and ease out fraud screening process.
- **Chargeback Guarantee**: In case of a fraud, such services fully cover approved orders which makes it a risk-free investment and safeguards money.
- **Device Fingerprinting**: A technique of recording information about the device a user uses when making online transactions. Multiple properties are analysed, including browser, operating system, location, language, etc., to find out whether the device used is related to fraud and can be blocked.
- **Customization**: Allows to manually customize fraud checks and data points to meet the nature of business and personal preferences.

9.1 Risk Management in online payments

Building an effective fraud risk management program requires solid understanding of how and why fraud is perpetrated. The risk of fraud is just one of the many types of risks to be managed by an organization. Without clear, defined objectives, a fraud risk management program cannot be effective. The foundation of a successful fraud risk management program is a well-designed and properly executed fraud risk assessment. The use of automated continuous monitoring tools is a best practice in managing the risk of fraud. However, if not implemented properly, it can become quite time consuming and cumbersome.

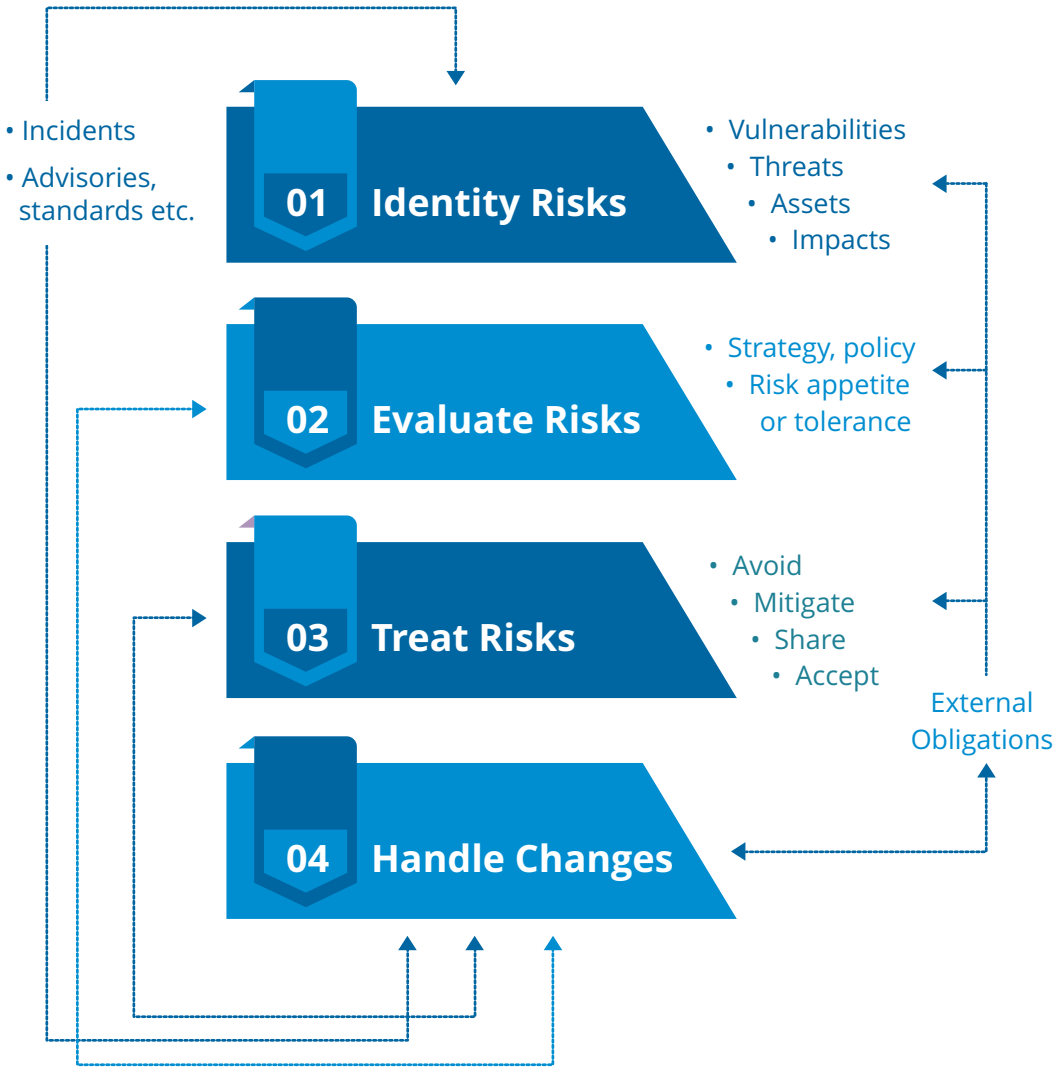
Risk management is a process of proactively and systematically identifying, assessing and evaluating risks with ongoing basis and chalking out plans and activities for treatment of the risks. This exercise is normally carried out by business entities who are looking to proactively improve their posture towards risks and threat prevention.

Risk management helps businesses identify potential threats, vulnerabilities and risks which when realized might materially harm the organization's interest. The organization then evaluates its possibility of occurrence and implements controls to treat the risk. The treatment could be to mitigate, transfer, accept or avoid the threats, based on the risk appetite and return of investment (ROI) for organization's business interest.

This process helps prevent frauds and related scams in retail payment transactions. This is a de-facto standard among organizations in payment industry. This is also mandated or encouraged by several regulatory and industry standard entities like PCI DSS, RBI, IT Act 2008, NPCI, etc.

[24] 10 eCommerce Fraud Prevention Tools to Stop Fraudsters; Template Monster; March 2018

Below is a typical risk management process diagram:



Part of the risk management includes playing out threat scenarios and evaluating possibility of impact and extent of damage on organizations' resources. This helps in identifying risk tolerance, building strategy and policies to treat risks. The risk management team then prepares possible ways to treat the risk. A host of external entities like auditors, advisories, penetration testers, standards are employed for the entire lifecycle of risk management. Risk management is normally not executed as point in time exercise but as an ongoing business as usual activity (BAU). This helps in learning from newer threats, technological changes in the industry and newer modus operandi by malicious and criminal entities.

The end objective and approach of the risk management exercise is to proactively prevent frauds from occurring in any of the entity in the digital payment ecosystem. Since the retail payment industry is interconnected and dependent, a threat in any one entity might result in fraud in a different organization in payment flow. For

example, a partial data leak in an issuer bank might result in large unauthorized transactions with a merchant. Currently, the entities in payment flow manage and treat risks within their organizations, and there is not enough infrastructure and ecosystem for exchange of potential industry threats and best practices between organizations at different levels.

Businesses across the globe implement security and risk management solutions primarily based on the solution provider marketing. The genuine reason for this is due to the integration and contractual challenges making it difficult to try before buy. Also, many a times the risk management leaders are held accountable for their decisions to buy a particular fraud management solution.

Risk management exercise, if made mandatory by respective payment regulatory and industry bodies, can help prevent frauds a large scale.

> Frauds committed on internet is still a fraud. The concept of fraud itself isn't new, it has always been around in one form or another. The rise of new technologies and payment methods have created new avenues for the fraudsters to commit new forms of fraud. In addition to customer awareness, businesses need to be equipped with necessary processes & tools to detect suspicious transactions as part of their fraud management efforts.
>
> **K N Yashvantha Kumar**,
> Deputy Superintendent of Police, Cyber Crime Division, Karnataka

10

RECOMMENDATIONS FOR VARIOUS STAKEHOLDERS

Retail Industry

The retail industry interacts with end consumers and handles most of the initial part of the payment transactions. The threat scenarios are fast changing, and the industry must keep up to protect themselves from frauds. Below are some recommendations to reduce and prevent frauds in this industry.

- Establish a fraud management framework that has discrete layers and measures that can be taken quickly taken to defend the frauds.
- Integrate data sources such as communication data, geospatial data with advanced modelling techniques such as machine learning, deep learning and natural language processing.
- Should have policies and procedures in place for forensic incident response, privacy, and customer management (to mitigate civil exposure).
- Should run logging functions to record evidence of irregular activities.
- Engage the Fraud and Risk Management teams starting from the early stages of product/feature development.
- Businesses should implement Key Performance Indicators (KPI) & Key Fraud Indicators (KFI) for fraud detection systems that would result in reduction in fraud loss and also reduction in false positives.
- Risk assessment – perform regular risk assessment on all its business landscape, including application architecture, back office operations, and personnel.
- In addition to the standard user authentication using credentials, advanced technologies that cumulate the data for passive device information, behavioural biometrics and network characteristics may be implemented.
- Review the existing fraud prevention & detection methods, and assess the likelihood that the existing methods can be subverted by the criminals
- Build a team involving from technology, security, legal, fraud risk management and user experience teams that work together as a team rather working in silos.
- Cross border industry collaboration to be established with merchants, issuers, acquirers, processors and other service providers to minimise online frauds
- Incorporate additional transaction verification methods for high risk/high value transactions.
- Regular internal and external audits & testing to help assess gaps and improve
- Disclose the information related to how the customer information will be used by the online retail payment systems to improve the customer trust.
- Proper structured implementation of business processes to handle fraud prevention systems to not miss out important alerts.

- Provide awareness to unsuspecting employees, consumers in countering the social engineering attacks including fraudulent behaviour, anti-money laundering, etc.
- Engage & educate consumers – educate customers and vendors on security practices and systems that are used in the products.
- A workforce trained and experienced enough to understand the difference between a fraudster and a genuine customer need to be built over time in anticipation rather than in reaction to events.
- Data analytics and machine learning help in reducing the reaction time and take proactive action.

Payment Industry

The payment industry consists of all the organizations which store, process and transmit payments and payment data, most notably credit & debit cards, as well as non-banking financial companies (NBFCs) managing wallets, UPI based interfaces, etc. The recommendations for payment industry are listed below.

- Compliance to standards – businesses must get audited and certified for standards like PCI DSS and ISO 27001
- Apart from compliance, regular internal and external audits must be performed to make sure the systems are safe and secure
- Protect stored cardholder data and encrypt transmission of cardholder data
- Enable continuous log monitoring and access management with the principle of least privilege
- Threat monitoring – perform active threat monitoring on its IT infrastructure to access potential threats and attacks and to block them
- Implement fraud management tools and encryption at payment gateways and endpoints
- Leverage advanced data analytics to enhance fraud detection and reducing the reaction time
- Adopt security and privacy first culture with adequate investments in cyber security to safeguard the payment technologies and process involved
- Have strong security and privacy by design principles and its adoption at the time of product development (inhouse and third parties/vendors and service providers) to mitigate issues at foundational level
- Consider implementing private or public bug bounty programmes to encourage developer community to find security exploits or vulnerabilities in their infrastructure

Policy Makers/Regulators

The card scheme networks (VISA, Mastercard, RuPay, etc), banks and government regulators come under this bracket. These entities control and manage most of the backend activities of the payment processing system. The processing systems, communication standards, operational techniques, etc., used in the industry are defined by these entities.

Following are the controls to be implemented by policy makers/regulators to prevent large scale frauds:

- Audit vendors and partners – include right to audit clause in agreements and regularly audit vendors and partners
- Standards development – develop standards for all aspects of payment processing systems
- Policy making – Engage with private groups, government entities and regulatory bodies and develop policies
- Threat modelling – Setup independent threat modelling systems that can detect anomalies and prevent frauds
- Build a govt. body that engages with private businesses and help them build secure products and services
- National policy and framework to protect nation's assets and citizens
- Improve laws and legal ecosystem to protect consumers and businesses
- Empower industry for Innovation and continuous development
- Engage with global partners
- Skill and threat information exchange with internal and external entities
- Provision for lateral entry of specialized cyber security talent in Govt. agencies and regulatory bodies
- Focused capacity building for employees in Govt. agencies and regulators in the area of cyber security
- Creation of a dedicated third-party that would engage in investigations related to frauds committed in online retail space. This entity should have quasi-police powers to investigate frauds.

Law Enforcement Agencies (LEA)

The law enforcement agencies, most of the time get involved in a particular case only when a breach or fraud has occurred. Also, the payment industry is evolving rapidly and thus the gap in skills and changing threat scenario makes it difficult for them during the fraud investigation and prosecution. Following are recommendations for LEAs.

- Empower and upskill prosecution and law enforcement agencies – industry, card network, and government must train and upskill LEA regularly
- Frequent training on basic structure and fundamentals of the payment industry as well as latest developments on technology platforms
- Investigation and forensic skills on payment industry must be regularly updated
- Engage with global players – engage with LEA of other countries, skill and threat information exchange with entities
- Regular LEA interaction with the industry
- Sensitize LEA on PII (personally identifiable information) and data privacy
- Training Data security and data protection controls in Payment industry

Consumers

Consumers have been generally the easy target for fraudsters to commit payment frauds. For consumers, it would be prudent for them to prevent frauds form occurring than have controls to investigate after they occur. Recommendations for consumers to prevent frauds at their end are listed below.

- Keep authentication credentials like OTP, password and even payment cards secure with them all the time. These should not be shared with anyone else or publicly.
- The payment cards – debit and credit itself can act as authentication credential and must be secured all the time. Because of the industry complexity, versatility, and implementation, payment transactions are processed differently. Some merchants, schemes and banks process transactions without additional parameter of authentication. Hence it is always recommended to secure the card itself.
- It is recommended to use devises like mobiles, tablets and computers from well-known and trusted vendors and OEMs.
- Always use licensed and trusted software and operating system on devices
- Use appropriate endpoint security programs like antivirus and firewall on devices. There are also tools like antimalware and anti-ransomware that provide advanced protection.
- Use caution in accessing trusted websites and portals for online transactions. Make sure all payment transactions happen on secure websites. Make sure the URL/address of the website is visible and is correct.
- Use caution while installing unknown software programs or apps on laptops or mobiles. Avoid unusual and untrusted apps to prevent password stealing or screen hijacking apps.
- Make sure only required permissions are giving to the apps on your mobile to prevent personal data leak.
- Be wary of phishing calls and messages. Do not share banking or personal information with untrusted persons.

> The Indian payment industry has a promising future and with increasing digitization in remote cities and rural areas, the digital payment adoption coefficient will be exponential.

This paper outlines the key components and recommendations to the payment industry, customers, law enforcement and regulatory bodies. The objective is to initiate discussions and develop solutions towards real-time fraud prevention and mitigation strategies.

Online payment safety is constantly being reinforced by Government laws and regulations backed by next-gen technologies to combat fraud. However, cybercriminals adapt quickly to changing dynamics and come up with new ways to perpetuate fraud. It is the combined responsibility to wake up and fight together against such organised efforts and safeguard the payment ecosystem. Future technologies must anticipate possible abuse and work towards baking security by design into the solution development lifecycle.

The COVID outbreak has proven that digital payments are the preferred choice and going forward, the dependency on digital infrastructure is only going to rise through every walk of life. Thus, awareness also forms an essential part of the fraud prevention strategy, right from educating consumers, training the workforce in the industry to equipping LEAs with necessary knowledge to mitigate risks.

In order to find the right balance between enablement and protection, it is critical that a collaborative effort be undertaken by all stakeholders involved, to establish a comprehensive fraud management framework for digital payments in India.

Acknowledgement

We would like to sincerely thank the efforts of everyone who has contributed and provided their valuable insights towards making this report a success.

A special mention to all senior police officers who took out time to provide their valuable feedback and recommendations which have been quoted in the report.

On behalf of DSCI & PayPal, we would like to express our gratitude to all the Law Enforcement Officers, Industry leaders and professionals, and external consultants for their valuable time and support without which this report would not have been possible.

Report Team

DSCI Team

K. Venkatesh Murthy
Director, DSCI

Suneet Pahwa
Deputy Director – Technical, DSCI

Amit K Ghosh
Manager – Communications, DSCI

PayPal Team

Nath Parameshwaran
Director, Corporate Affairs, PayPal India

Phoram Mehta
Senior Director, APAC CISO, PayPal Inc.

Mangesh Samant
Tech & Security Oversight Manager, SEA & India, PayPal

Vaibhav Gupta
Director, Commercial Seller Risk, PayPal

Special Acknowledgement

Niranjan Patil
OPSEC Inc

Naren Shivappa
Ominaya

Pranesh Joshi
Ominaya

About DSCI

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM®, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

For more information, visit: **www.dsci.in**

About PayPal

PayPal Holdings, Inc. (NASDAQ: PYPL) is committed to democratizing financial services and empowering people and businesses to join and thrive in the global economy. Their open digital payments platform gives PayPal's 227 million active account holders the confidence to connect and transact in new and powerful ways, whether they are online, on a mobile device, in an app, or in person. Through a combination of technological innovation and strategic partnerships, PayPal creates better ways to manage and move money, and offers choice and flexibility when sending payments, paying or getting paid. Available in more than 200 markets around the world, the PayPal platform, including Braintree, Venmo and Xoom, enables consumers and merchants to receive money in more than 100 currencies, withdraw funds in 56 currencies and hold balances in their PayPal accounts in 25 currencies.

For more information on PayPal, visit: **https://www.paypal.com/about**

For PayPal Holdings, Inc. financial information, visit: **https://investor.paypal-corp.com**

DATA SECURITY COUNCIL OF INDIA

NASSCOM CAMPUS, 4th Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

For any queries, contact:

P: +91-120-4990253 | E: info@dsci.in | W: www.dsci.in

DSCI_Connect | dsci.connect | dsci.connect | data-security-council-of-india | dscivideo

PayPalIN | PayPalIN | paypalindia | PayPal | PayPalIndiaOfficial