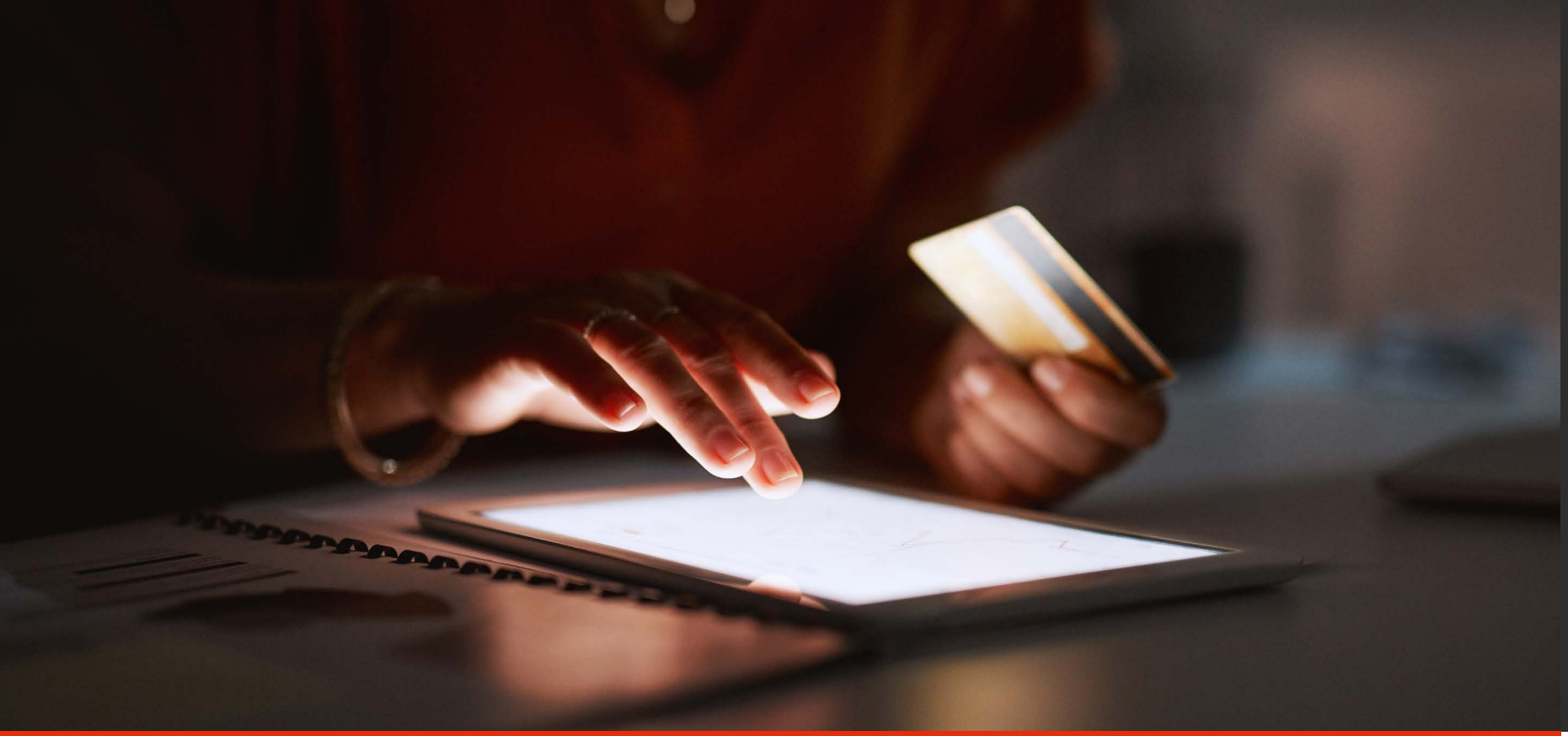


Combating fraud in the era of digital payments

May 2022

pwc

Click to launch

Foreword

Dear readers,

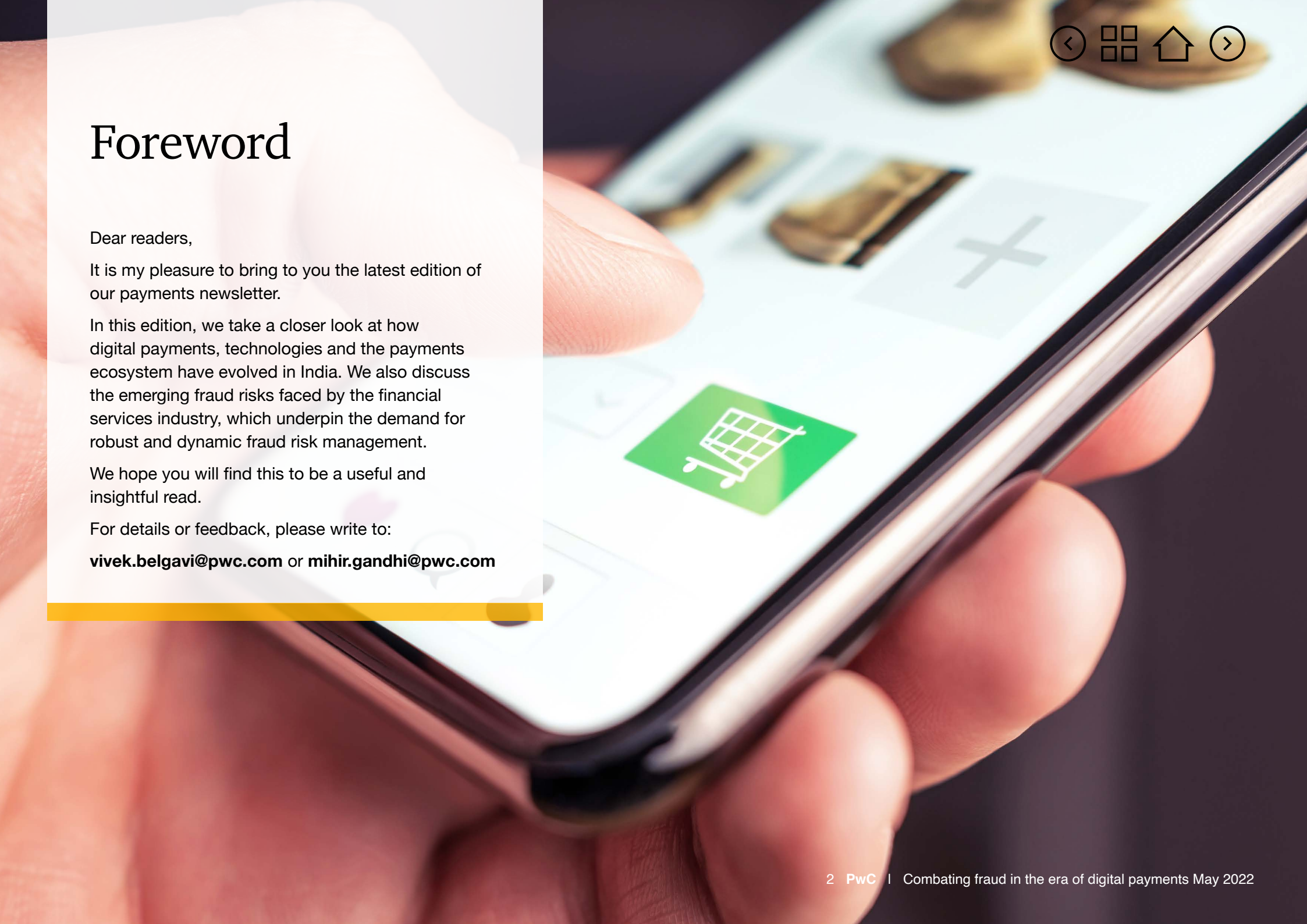
It is my pleasure to bring to you the latest edition of our payments newsletter.

In this edition, we take a closer look at how digital payments, technologies and the payments ecosystem have evolved in India. We also discuss the emerging fraud risks faced by the financial services industry, which underpin the demand for robust and dynamic fraud risk management.

We hope you will find this to be a useful and insightful read.

For details or feedback, please write to:

vivek.belgavi@pwc.com or **mihir.gandhi@pwc.com**



In this issue

01 Introduction

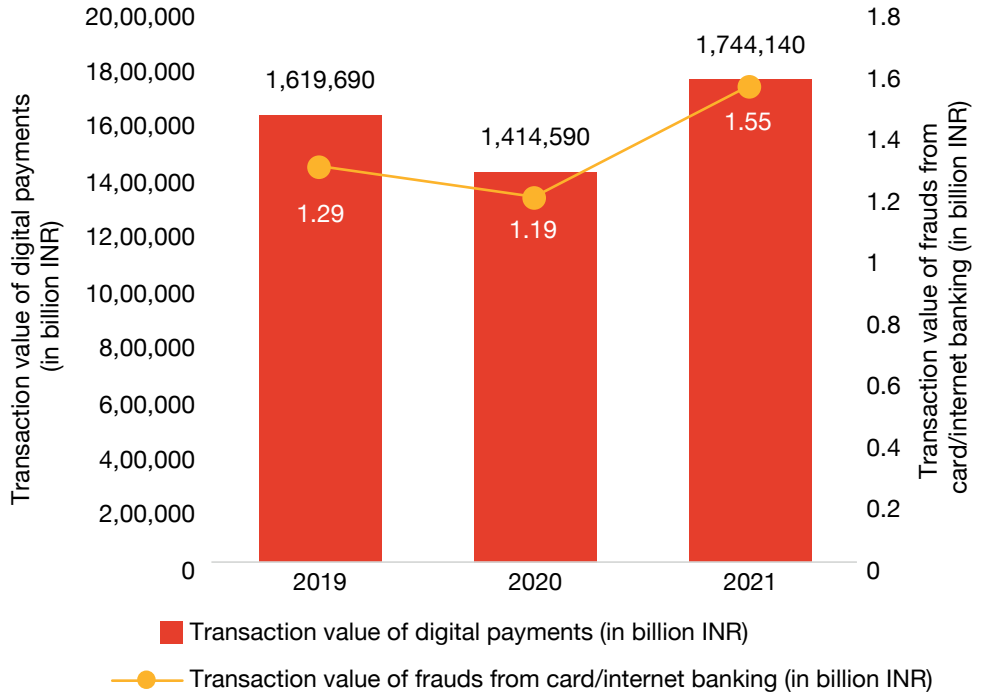
In the last few years, especially post demonetisation in 2016 and the COVID-19 pandemic, there has been a major spike in the number of digital payments in India. Innovation in the payments landscape, regulatory support, the increase in smartphone penetration and cheaper mobile internet access have played a key role in the adoption of digital transactions and their rapid growth in India. Payment service providers, along with new players and additional investments, have been providing an enhanced seamless user experience at competitive prices, promoting wider adoption of digital payments.

Users have multiple options for digital payments such as cards, wallets, Unified Payments Interface (UPI), mobile banking, QR code and various other methods. UPI has contributed significantly to the growth of digital transactions in India. In 2021–22, UPI accounted for a record 46 billion transactions out of the total volume of 72 billion digital payment transactions.[1] This number was an increase of 109% over the previous year's volume of 22 billion. Digital payments grew by 64% during the same period.

The increase in the adoption of these advanced payment options, however, has also generated unprecedented opportunities for fraudsters to perpetrate fraud by exploiting digital payment systems and human vulnerabilities.

As per the Reserve Bank of India's (RBI) Annual Report 2021–22, the volume of frauds reported by financial institutions (FIs) using cards and internet banking was 34% higher at 3,596 in 2021–22 as against 2,677 frauds in 2019–20. The value of fraudulent transactions in 2021–22 was INR 1.55 billion – 20% more than that in 2019–20 (INR 1.29 billion). In terms of value, these card- and internet-related frauds amounted to 0.2% of the total value of fraudulent transactions. Overall, the payment frauds as a percentage of total digital payments in India has increased from 0.008 bps in 2019–20 to 0.0089 bps in 2021–22.

Value of frauds vis-a-vis the digital payments transactions (cards and internet banking)



1 RBI Annual Report 2021–22

With the rise in technological advancements, incidents of fraud have also become more organised and sophisticated – for example, targeted hacking into networks and databases, phishing attacks, etc. This has become a major concern among consumers. Specifically, with significant data relating to cards being stored and transferred digitally, fraudsters can attempt to exploit vulnerabilities in the system and gain access to such information for wrongful use.

The changing nature of fraud and increase in fraudulent activities can be attributed to the following factors:

1. **Diversified entry points:** Businesses in India have been digitising across their value chains at breakneck speeds. This increases the scope of opportunities for fraudsters and offers them a wider attack surface for exploitation. The common entry points include social media, e-commerce, or services like retail transactions, rideshares and lodging.

2. **Vulnerabilities in the new payment technologies:** Due to the expanding digitisation of businesses amid growing competition, the payments industry has come up with multiple payment platform options for customers. However, platforms with weak server-side controls make the payments infrastructure vulnerable to attacks.

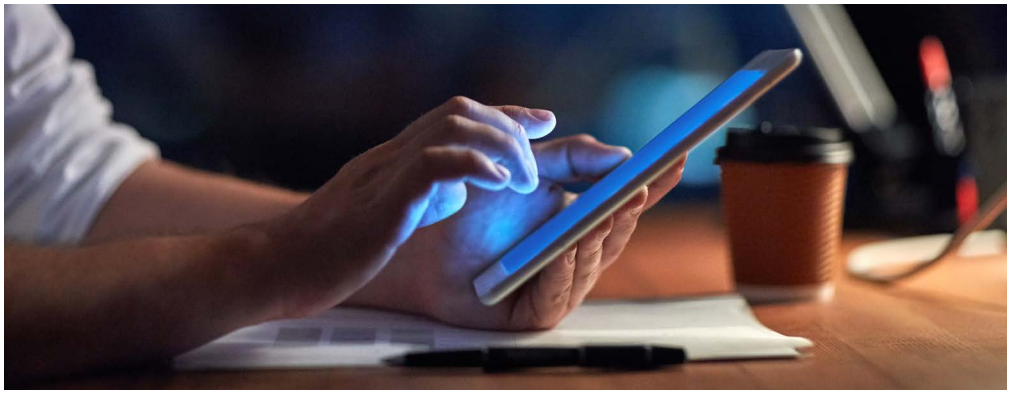
   Further, the risk of cyberattacks has increased significantly due to more data records – personal and financial information – being stored digitally, and employees connecting remotely through unsecured networks. Customers are also increasingly falling prey to the 'authorised' push payment fraud in the new payment technologies.

3. **Lax preparedness of new players:** There are multiple new-age digital native start-ups entering the ecosystem, with a lot of customer data at their disposal. However, they lack the wherewithal to handle the much-needed security aspect.

4. **Lack of customer awareness:** Despite increased efforts by payment service providers at customer education, customers often become victims of fraud very easily. This can be attributed to their lack of awareness of the new and advanced payment technologies and fraud tactics associated with them.

5. **Unsecured remote access:** With the advent of work from home in the pandemic era, organisations have become more susceptible to payment data leaks owing to remote access to their systems. Default credential setting and open remote access has now become easier outside the firewalled confines of an organisation, thereby helping fraudsters to take control of devices and engage in fraudulent activities.

The advanced techniques used by fraudsters impact customer trust in digital payment instruments. For FIs, fraud may lead to loss of reputation and huge liabilities. Therefore, it is of utmost importance to mitigate and prevent such incidents. Having risk mitigation measures in place can significantly reduce exorbitant operational costs. Such measures eliminate the need to spend time and resources on reviewing every transaction alert. Moreover, these measures safeguard a company's reputation and, in turn, its customer base, helping it to avoid regulatory actions.



02 Fraud in digital payments

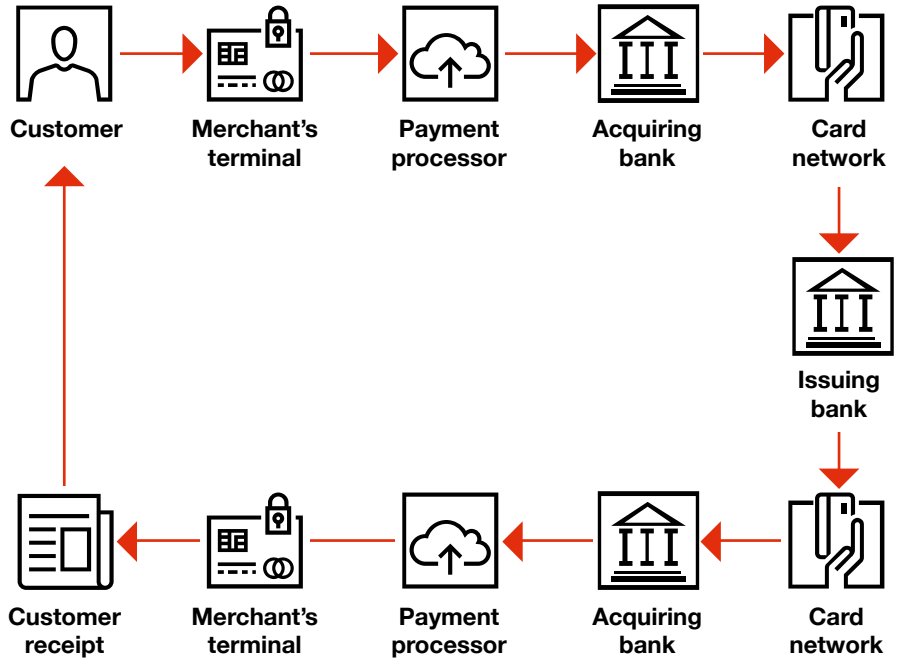
Frauds, in any country, are driven by multiple factors such as local payment behaviour, customer awareness, security of payment systems, the regulatory environment, maturity of the payments domain, technical advancements and economic development of the country.

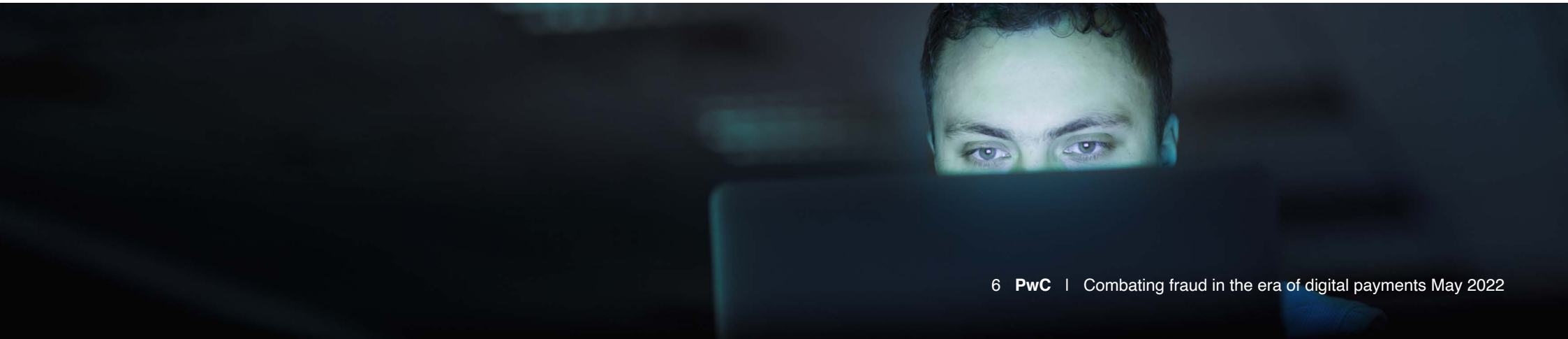
The payments ecosystem comprises multiple stakeholders such as banks, networks, payment gateways, channels, sellers, merchants, customers and buyers, which interact with each other. These stakeholders may have risks associated with them.

For example, a single payment from a customer to a merchant involves multiple stakeholders in the payments process flow. When the customer pays the merchant, the relevant information is passed on from the merchant payment gateway and processor to the customer's issuing bank, through the card association network. Once the customer's issuing bank authorises the transaction and deems it valid, the payment processor completes the transaction.

During this process, frauds can be perpetrated at any stage. Some common techniques and tricks used by the fraudsters in perpetrating these frauds across the payments ecosystem have been detailed in the following section.

Payments processing cycle using a card





1. Common fraud typologies

The RBI's Annual Report 2020–21 suggests a clear increase in the number and value of payment frauds in India. The frauds and mitigation measures for the same have been covered in a press release by the RBI.[2]

In the following section, we take a closer look at the common fraud typologies in an Indian context, including common tactics used by fraudsters, along with the payment instruments or channels that are most vulnerable to these types of frauds.

1.1 Identity theft/impersonation

Fraudsters acquire users' personal information (e.g. PAN/Aadhaar details or social media credentials) or critical information about their bank accounts in order to gain access and initiate online payments or open a payment account to execute transactions. Personal data of customers is made available on the dark web, enabling fraudsters to carry out this type of fraud. There have been multiple incidents in India involving banks, payments banks and other FinTechs wherein the victims of identity theft have reported that their personal details were used by fraudsters to perform fraudulent transactions, including availing of credit card facility from banks.[3]

Fraudsters may also impersonate an authorised official (bank employee, police, Government official, health official, etc.) or the user's trusted acquaintance, and manipulate the user into transferring money.

1.2 Phishing/vishing

In India, as the adoption of digital transactions has become more widespread, there has been an increase in the number of phishing and vishing frauds. Fraudsters execute vishing frauds by posing as customer service executives from banks and convincing the unsuspecting customers to complete or update their electronic Know-your-Customer (eKYC) online in order to keep the account active. When the customer performs the process online, the fraudsters obtain confidential information and manage to perform illegal transactions using the OTP shared. Also, the fraudsters do not let the customer hang up the phone lest he/she should come to know about the illegal transaction.

In phishing frauds, the fraudsters send emails or text messages that contain a malicious link which takes the customer to a web page that is deceptively similar in appearance to the actual website of the bank. The customers end up mistaking the fraudulent website for the actual one and enter confidential information, which is then used by the fraudsters to perform illegal transactions.

1.3 Web skimming

Web skimming is a hacking technique wherein the fraudsters install malicious software on the payment or checkout pages of an application and obtain confidential payment information. For instance, e-commerce websites employ use of third-party applications, paving the way for fraudsters to install their malicious code into the trusted third-party host site.

There have been multiple reported cases of web skimming in India where fraudsters obtain the card details – such as card number, CVV and expiry date – of unsuspecting users through e-commerce websites. The e-commerce websites have been particularly targeted due to their popularity and widespread presence.

2 https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs PR163037E920A47573411FBC7D79B058FED34A.PDF

3 https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf

1.4 By using QR code

The number of Bharat quick response (BQR) codes deployed in India in 2020–21 (49.7 lakh) have increased by 39.3% from 2019–20. At the same time, fraudsters have exploited the use of QR codes for conducting fraudulent transactions.

In many cases, fraudsters send a fake QR code to the unsuspecting customer, scanning which will enable the customer to receive money in his/her bank account. However, once the code is scanned, the money gets deducted from the customer's account instead. Also, in some cases, the fraudsters replace the physical QR code with their own QR code at shops/merchant locations, thereby deceiving customers to make payments to the wrong account.

1.5 Social engineering

Social engineering attacks generally involve exploiting unsuspecting users by convincing them of a serious issue related to their bank accounts so that the users divulge confidential information. In most cases, the fraudster psychologically manipulates the unsuspecting user into divulging their banking details or convinces them to make payments. The perpetrator generally pretends to be from a trusted organisation or poses as a family member of the user or an employee of an FI.

1.6 Account takeover

This type of fraud involves fraudsters trying to take illegitimate control of the user's account by stealing their login credentials and making payments. In most cases, the fraudsters remain unnoticed as they change the details obtained at the first step, before performing payments.

1.7 Database breach

Fraudsters, or a group of organised criminals, gain access to the banking systems or payment service provider networks to initiate or alter transactions. The 2016 cyberattack[4] on the Bangladesh Bank, Central Bank of Bangladesh, is a classic example, where organised criminals got access to the bank's credentials and authorised payment transfers.

1.8 Remote access assistance

In this type of fraud, the fraudsters convince the user to provide remote access to their device for resolving some technical issues. They often do so by impersonating a member of a laptop servicer's technical support team, or a bank official helping to unblock the user's account or provide KYC support. After gaining remote access, the fraudsters gather all confidential information related to the user's payment accounts and misuse it to make payments.

Several cases have been reported where people receive an SMS asking for the KYC update of their bank account, along with a number to call for assistance. When people call for assistance, the fraudsters ask them to download a remote support application and share a code to receive confidential information and siphon off money from the bank account.[5]

1.9 Botnet attack

Fraudsters inject malicious software (also known as bots) into a group of computers and link them together to launch coordinated botnet attacks. This allows fraudsters to gain access to the user's devices, and override their existing security methods to record the user's sensitive information. Later, this information is used to conduct fraudulent activities.

4 https://www.rbi.org.in/scripts/FS_Speeches.aspx?Id=1022&fn=2

5 https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR163037E920A47573411FBC7D79B058FED34A.PDF

Several incidents have taken place where botmasters gained access to private shopping data across various brands and personal computers using bots. These bots are downloaded by an unsuspecting user via pirated software, advertising links, email attachments, etc.

These are some of the common and emerging fraud typologies and methods used by the fraudsters to target various digital payments channels used by FIs in India. Incidents of fraud in digital channels have been on the rise when compared with those in conventional channels. The risks of conventional channels are widely known, and people are aware of the methods to protect themselves against such frauds. However, they lack the experience and awareness when it comes to newer or digital channels.

2. Use of fraud typologies to perpetrate payments channels

As discussed in the previous section, fraudsters make use of various methods and techniques to carry out malicious activities using various payments channels in India. These activities are often aimed at attacking the payments infrastructure and result in financial losses. Some of the payments channels used by fraudsters are listed below:

2.1 UPI payments and wallets

UPI offers multiple payment flows such as QR code scanning, UPI ID-enabled payments or phone number-based payments. Fraudsters often employ various methods in order to trick unsuspecting users. A common method involves sending the user a malicious link guised as a collect request to pay for a product/service.

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

Other common fraud methods used in UPI payments include fraud by using fake QR codes and remote access assistance.

2.2 ATMs /point-of-sale (PoS) machines

By using personal data obtained via remote access assistance or skimming devices installed at ATMs/POS machines, fraudsters execute transactions from the user's account. In addition, fraudsters may claim false chargebacks using cards. The common types of fraud perpetrated in ATMs/PoS machines include card skimming and unauthorised access.

2.3 Aadhaar-enabled payment system (AePS)

AePS is another mode of payment wherein customers use their Aadhaar for identification at a business correspondent (BC) equipped with a biometric POS in order to perform cash withdrawals. Corrupt BCs can withdraw more than the amount the customer has requested without providing a receipt, and siphon the excess amount. Fraudsters can also clone the fingerprints (biometrics) of customers and withdraw money from the AePS.

Several cases of fraud involving siphoning of Government welfare funds meant for underprivileged beneficiaries using AePS have surfaced in the recent past in the country. Most AePS-enabled frauds are perpetrated due to customers' lack of knowledge and awareness regarding the use of AePS. Fraudsters also hack the database and get unauthorised access to the customer information and perform fraudulent activities through AePS.

2.4 Internet banking

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

2.5 Mobile banking

With an increase in the availability of smartphones and internet penetration, mobiles phones have become the most opted instrument to perform digital transactions. Users have the option of downloading the applications of banking service providers on their mobile device to perform such transactions easily. However, as such channels are vulnerable to fraud, the fraudsters can misuse the user's credentials or personal data to penetrate into the user's banking application.

2.6 Prepaid cards

Stolen prepaid card information can be easily used by the fraudsters to make transactions or buy a prepaid card with stolen payment credentials. Prepaid cards preloaded with money are often not linked to any account. Thus, they cannot be tied to any specific user, which makes them vulnerable to fraud.

3. Future fraud risks

The advancement of new-age technologies has taken the delivery of financial services and the customer experience to the next level. FIs are actively using artificial intelligence, machine learning, big data and natural language processing to redefine their products, service delivery models and the overall customer engagement. However, these emerging technologies are not immune to fraud risks. A few potential fraud risks associated with these technologies are detailed below:

3.1 Frauds related to near-field communication (NFC) technology:

NFC-enabled cards for contactless payments are comparatively more secure as they employ radio frequency waves instead of internet connectivity. However, one major drawback associated with such cards is the lack of password protection. Fraudsters will exploit this technology as the payment acceptance limit on such transactions continues to increase.

3.2 Cryptocurrency frauds:

With the increasing public interest around cryptocurrencies, it is only expected that this currency will also be susceptible to malicious attacks and be exploited by attackers and cybercriminals. According to a report released by the Federal Trade Commission (FTC) consumer sentinel,[6] scams in crypto are seeing an exponential rise in the United States, with losses of around USD 80 million from Oct 2020–Mar 2021, which is ten times that of the previous year. The most common and emerging cryptocurrency frauds can be classified as below:

a. Investment scams:

With little knowledge of the digital currency market, users or investors are easily tricked into believing the authenticity of a cryptocurrency. New types of coins are introduced every day and released in the market as an initial coin offering (ICO). Fraudsters are creating fake websites that draw investors in these currencies with the promise of substantial returns. As more and more investments come in – inflating the value of the currency – the initial investors pull out their holdings in an act frequently termed as a 'rug pull'. Once the scammer's money has been pulled out, the platform is taken down, leaving investors with no option to sell their assets.

b. Wallet scams:

There are two types of wallets in the crypto world, commonly distinguished by the mode of storage of the currency – online or offline. These are known as hot and cold wallets respectively. Hot wallets are susceptible to potential phishing scams, whereas cold wallets are susceptible to loss of currency when the storage device is lost or the passkey to access it is forgotten.

Phishing scams related to crypto wallets are similar to those involving other types of wallets. In both cases, fraudsters try to retrieve personal

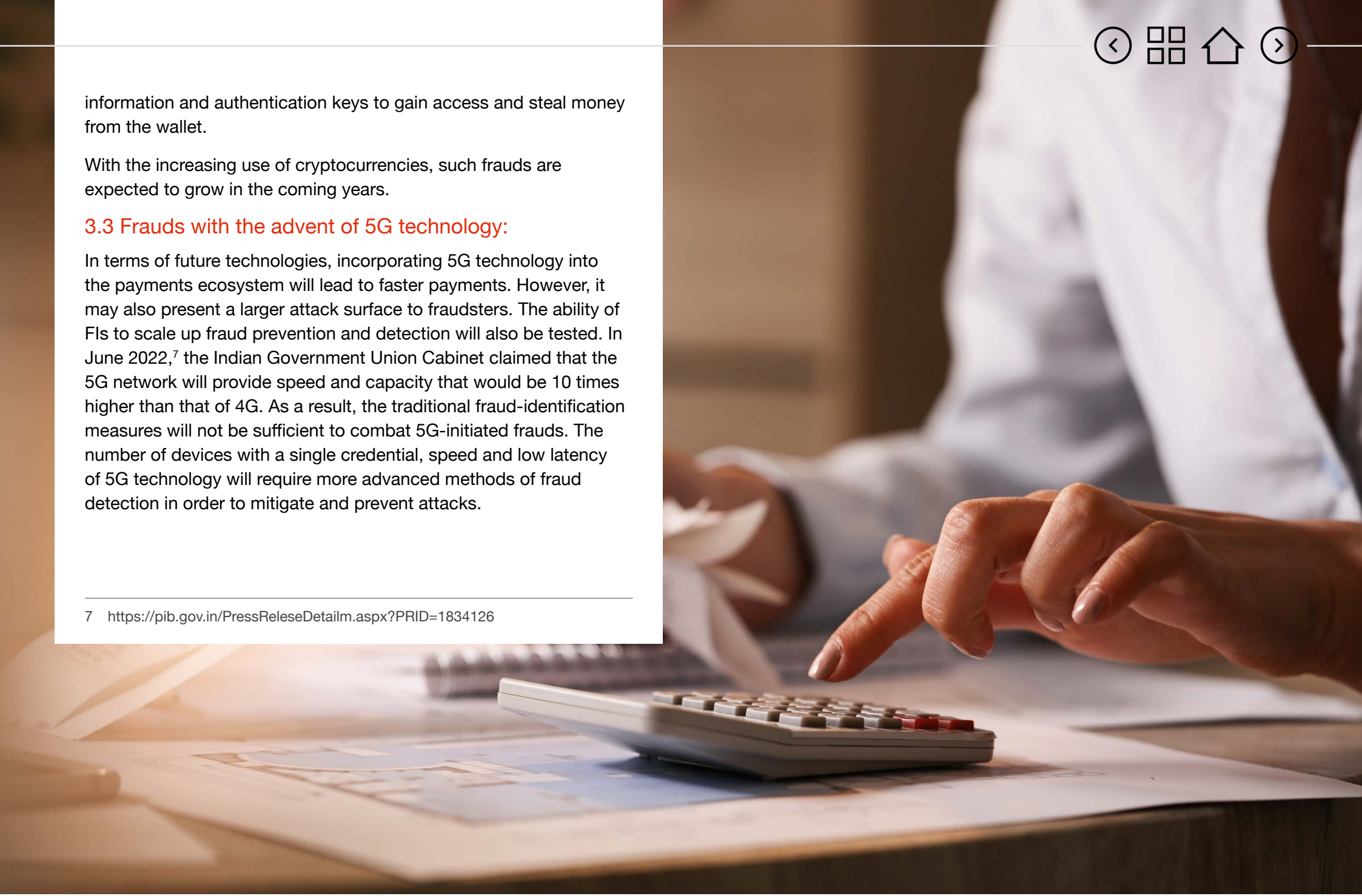
6 https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-data-shows-huge-spike-cryptocurrency-investment-scams

information and authentication keys to gain access and steal money from the wallet.

With the increasing use of cryptocurrencies, such frauds are expected to grow in the coming years.

3.3 Frauds with the advent of 5G technology:

In terms of future technologies, incorporating 5G technology into the payments ecosystem will lead to faster payments. However, it may also present a larger attack surface to fraudsters. The ability of FIs to scale up fraud prevention and detection will also be tested. In June 2022,[7] the Indian Government Union Cabinet claimed that the 5G network will provide speed and capacity that would be 10 times higher than that of 4G. As a result, the traditional fraud-identification measures will not be sufficient to combat 5G-initiated frauds. The number of devices with a single credential, speed and low latency of 5G technology will require more advanced methods of fraud detection in order to mitigate and prevent attacks.



7 https://pib.gov.in/PressReleseDetailm.aspx?PRID=1834126

03 Fraud risk management

FIs have started taking a holistic approach towards fraud risk management by gradually shifting from static and standalone fraud detection and monitoring systems to a dynamic enterprise-wide fraud risk management approach that supports them throughout the life cycle of customer transactions. The pandemic increased the volume of digital payments. As a result, the evolving multiple channels of customer engagement and accelerated adoption of new technologies in payments have had a profound impact on how an FI manages its fraud risk.

FIs are increasingly adopting a framework that integrates the people, policy and process, and technology aspects together for a more effective, agile and dynamic anti-fraud response.

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

The end-to-end fraud risk management response of an FI must balance customer experience with fraud control priorities. However, managing fraud risk while improving the customer experience is a major challenge faced by FIs amid the evolving payments landscape. The key aspects of fraud risk management are explained in detail below:

1. People

1.1 Dedicated fraud control unit (FCU)

FIs should have a dedicated and independent fraud control unit staffed with resources having skills and experience in fraud risk management. Knowledge of all business units, products and services, technologies involved, and complexities of business is equally important for the FCU staff. Specifically, the FCU staff should be familiar with technology, fraud risk and security.

1.2 Regular training and awareness

The FCU staff need to get regular training and attend awareness sessions on fraud risk management. This training should cover the following areas:

- governance framework, policies and procedures to prevent and detect fraud risks
- updates on new payments channels and the specific risks associated with them
- traditional and emerging fraud risks
- technologies used by FIs for fraud prevention and detection
- fraud detection methods and techniques
- fraud reporting for internal and regulatory compliance perspective.

In addition, an FI should look at the following aspects:

- The audit committee and board of directors should have sufficient oversight of the management's anti-fraud programmes and controls.
- The personnel in the FIs should respond in a timely and appropriate manner to significant control deficiencies, allegations or concerns of fraud, and violations of the code of ethics/conduct.
- The organisation must have an accountability and authority matrix (RACI matrix), and people should be assigned responsibilities to mitigate fraud risks.

1.3 Customer awareness

FIs must adopt nuanced measures to enlighten their customers and make them aware of new digital payments channels, products, fraud risks and how to safeguard their payments. As per regulatory directives, FIs should create relevant usage guidelines and training materials for customers to help them use their products. They should also provide all details regarding the process to complain about a digital product or to report any fraudulent or suspicious activity in the account immediately. Moreover, FIs must ensure that their customers are aware of the types of threats that could occur while using digital products and know how to take necessary precautionary measures. Information about the common fraud techniques – such as phishing, vishing, remote access and account takeover – used by criminals to gain fraudulent access to payment and sensitive information about customers must also be provided. Such training and customer awareness programmes will help people to understand the ongoing security concerns in the payments ecosystem and how to minimise fraud risks by staying alert.

It is also important that the customers read the mandated agreements and agree to the terms and conditions before using any payment product and remain vigilant.

2. Process

2.1 Fraud risk governance framework

Setting up a fraud risk governance framework entailing the tone at the top, strategy, risk appetite, roles and responsibilities, accountability fraud mitigation, and fraud reporting is crucial for any FI. The fraud risk management policies and procedures should comprehensively:

- define the fraud risk drivers for FIs (product and services risks, channels, etc.)
- set risk mitigation controls (preventive and detective) in transaction monitoring, risk assessment and testing
- facilitate reporting and customer management.

2.2 Risk assessment

It is important for an FI to assess the likelihood and impact and mitigate the fraud risks associated with its business, products and services, and channels. Different areas of business are susceptible to different levels and types of frauds. A typical fraud risk assessment exercise of an FI would involve conducting a detailed assessment of its:

- business risks
- customer risks
- product and services risks
- technology risks
- channel risks
- employee-related risks.

Every new product should undergo a fraud risk vulnerability assessment. For example, fraud risks associated with a new digital account-opening service should be assessed in detail before its given a go-ahead.

Regular fraud risk assessments will provide FIs with the understanding to tailor their anti-fraud programmes in order to mitigate emerging threats, improve customer experience and complement and support business growth.

Overall, the fraud mitigation framework should help an FI identify, prevent, detect and respond to fraud risks. This will also help the organisation to reduce the overall cost of managing fraud risks.

To summarise, FIs need to check that they:

- have a formal and regularly scheduled procedure to perform fraud risk assessments
- assess the design and operating effectiveness of anti-fraud control activities.

2.3 Fraud simulation testing

Fraud simulation testing is another proactive measure to assess the process and system's vulnerability to fraud risk. Pseudo fraud scenarios are developed based on the emerging fraud risks and simulated on actual, select transactions to assess if the monitoring controls can detect them.

2.4 Investigation and reporting

An independent incident response or investigation team as part of the FCU with investigation skills and experience is key for investigation, identification of control breaches and liaison with regulatory and law enforcement agencies. The team should have knowledge of the current and emerging channels and products. Also, the team should be proactive, and report new risks and frauds identified to senior management on a timely basis. This can be done by leveraging the data obtained from the risk assessments conducted.

3. Technology

Having a technology-enabled risk management system ensures easy identification, management and further mitigation of frauds. Below are some of the technology-enabled measures that FIs can adopt for better fraud risk management.

3.1 Advanced analytics

With the help of behavioural analytics, data of the known frauds, customer behaviour, risk and transaction profile can be translated into scenarios to monitor the risks effectively by reducing the response time.

3.2 Real-time monitoring

Traditionally, rule-based systems were used to detect fraudulent transactions. However, this methodology yields a high number of false positives, which impacts customer experience due to the long lead times required to prove the authenticity of transactions. In this era where transactions happen in milliseconds, having a real-time fraud detection system becomes a necessity for firms operating in the financial sector. Such a system would help in proactively identifying potential security lapses caused by hackers and fraudsters, and block such transactions to ensure the safety of customers.

Technology plays a pivotal role in real-time monitoring of transactions and subsequent detection of fraudulent activities. AI-/ML-enabled technology systems, along with the rules and scenarios driven by analytics, play a crucial role in proactive risk identification and mitigation in real time while balancing the superior customer experience of a seamless transaction.

3.2.1. Dynamic customer data monitoring

FIs can leverage AI, ML data-driven techniques and high-performing analytical models that work on in-memory computing and use dynamic customer data – such as customer behaviour, profile updates transaction pattern and services availed – to visualise the hidden data patterns and create a risk management tool to highlight the anomalies in the payments.

Data used to build the models is not limited to the transaction data available with FIs. FIs also leverage third-party services to get customers' non-transactional data such as utility payments, salary statements and credit scores to build a 360-degree view of the customer. Hence, this approach will have higher accuracy in flagging any abnormal activity when compared to a traditional rule-based system.

3.2.2. Multi-factor authentication and biometrics

Embedding additional security features such as multi-factor authentication and biometrics during the product design and development stage is effective in ensuring the security of payment systems.

3.2.3 Device monitoring:

FIs can conduct transaction monitoring using device legitimacy monitoring which involves keeping track of the device IP, device geolocation, etc. Such identification techniques add a layer of security to real-time fraud scoring of a transaction. Such methods analyse information related to the device the transaction is requested from and flag any abnormal activity such as a new device login, login from an unusual location, configuration of the device, and IP address changes. This monitoring helps in proactively reaching out to customers to verify transaction authenticity, thereby reducing the associated payment risks. Before setting up a fraud monitoring tool, it is important for an FI to consider the following:

- whether the fraud monitoring tool is integrated with all data sources
- whether the fraud monitoring tool implemented is used to detect financial stress/potential fraud across all channels and services
- whether the fraud monitoring tool is configurable – based on financial and non-financial parameters
- whether the fraud monitoring tool has data transformation capabilities (has functionalities around how data from various sources should be transformed/enriched to run the analysis).

Regulatory initiatives for fraud prevention and detection

Regulators in India have also been engaged with FIs in understanding the data and challenges, and supporting a technology-driven framework for effective fraud risk management. There are guidelines for fraud prevention, detection and fraud reporting. The Central Bank regularly publishes guidance for the entities operating in the payments ecosystem to help curb frauds. The RBI master circular for fraud risk management in digital payments is one such recent regulatory guidance. It provides FIs with certain key factors and parameters that they need to consider as part of their fraud monitoring function. Reporting to the Central Payments Fraud Information Registry (CPFIR) is another measure by the RBI to gather insights and data from the industry on frauds, which enables better regulatory framework and decision making regarding fraud monitoring. Regulators also conduct regular workshops to raise fraud management awareness.

Likewise, a group of organisations or industry specialists define industry standards such as Payment Card Industry Data Security Standard (PCI-DSS), Payment Application Data Security Standard (PA-DSS), and ISO27000. FIs are expected to abide by these regulations, standards or policies, as well as have internal policies or frameworks in place to prevent, detect and combat frauds.

04 Conclusion

Based on the fraud trends over the past few years, FIs must adopt a dynamic fraud risk management framework that balances risk management and customer experience. Further, as FIs adopt new channels for customer engagement, launch new products and services and make new alliances, the alignment of the fraud risk management process, data and systems and the integration of all of these elements will enhance the overall customer experience. Therefore, embedding the fraud management process into overall customer engagement and experience should be the first step forward.

The rapid adoption of new-age payment instruments continues to pose security challenges to FIs. To protect themselves and their customers, FIs must have an agile fraud risk management framework and invest in newer and safer tools and technologies.

Safety of digital payments, assessment of anti-fraud controls, and collection of fraud data to analyse patterns and red flags have been emphasised by the regulators and law enforcement agencies along with the use of new technologies to mitigate fraud risk. The pandemic and increased penetration of internet and mobile phones have only accelerated the use of digital payments, and the dependency on them will continue to increase in future. Thus, spreading knowledge and awareness of new payment technologies, channels and products, and the risks involved – to both customers and employees – is a crucial part of a fraud prevention strategy.

Effective fraud management requires a combination of different measures along the payment value chain. FIs are using fraud orchestration techniques in parallel with their prevention, detection and response measures. Fraud orchestration helps FIs mitigate fraud holistically by providing a comprehensive view of the situation at hand. This is done by gathering information from all payment channels, creating a transparent interface, analysing the payments information using the latest technology, and helping to manage fraud by letting the investigation team take appropriate decisions. This process helps define automated strategies for a better fraud risk management framework.

It is important for FIs to understand the basic building blocks of any payments ecosystem in order to be able to ask the right questions for mitigating fraud and work on the three key elements – people, policy and process, and technology. Also, it is important to continuously review the framework and perform risk assessments to update risk profiles and controls for fraud mitigation.

Payment fraud threats have provided a useful opportunity to FIs to strategically collaborate with technology firms offering new-age solutions in areas related to security, data privacy and fraud risk management. These firms leverage the power of big data, AI and advanced predictive modelling to detect security risks and frauds at various touchpoints in the payments life cycle and help to mitigate them.

As a popular saying goes, ‘risk cannot be eliminated, it can only be mitigated’. Therefore, it is necessary for FIs to continuously assess risks and provide a secure and future-ready transaction environment to customers.

Contact us

Vivek Belgavi
FinTech and Alliances Leader
PwC India
vivek.belgavi@pwc.com

Mihir Gandhi
Partner and Leader, Payments Transformation
PwC India
mihir.gandhi@pwc.com

Dhruv Chawla
Partner, Advisory Services
PwC India
dhruv.chawla@pwc.com

Contributors

Induvant Tomar, Neha Dharurkar, Mayank Tiwari, Rohit Mishra, Shashank Gupta, Nishi Sureka, Manvitha Syamala

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 156 countries with over 295,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

pwc.in

KS/June 2022-M&C 20526