Unlocking the power of digital payments through security

ASSOCHAM
Ideate · Innovate · Impact

EY
Building a better working world

Table of Contents

FOREWORD

Sumant Sinha
President, ASSOCHAM

FinTech innovations and digitization are key enablers to achieve financial inclusion by extending financial services to the large un-served population of the country, unlocking huge growth potential. Today technology advancement in the space of the financial sector ecosystem is changing our lives significantly. Increasing digitization of core business processes through extensive use of internet technologies, shifting attention to mobility and deployment of many evolving technologies, have been reshaping the financial sector. Cybersecurity of financial transactions and its associate operational infrastructure are of prime importance. Given the accelerated adoption of digital payments and making India cashless, the nation warrants a special focus on financial sector cybersecurity posture.

Rapid digitization has always been one of the core objectives of the 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. Overall rise in digitization threats in India requires various stakeholders, including government, industry leaders and law enforcement agencies, to come together to ensure robust cybersecurity posture, especially around digital payments. International cooperation is required to develop robust cybersecurity measures through enabling policies and protocols.

The Reserve Bank of India launch for the first pilot for retail digital Rupee or e-rupee is a remarkable step for banking industry. With the digital Rupee, the broader wish of the central bank is to execute a full-fledged launch of the CBDC (central bank digital currency) in the near future. With these developments happening in BFSI segment, I am glad that ASSOCHAM is organizing the Digital Financial Security Conclave 2022. ASSOCHAM and EY have collaborated on preparing a joint report on Digital Financial security 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 toward economic prosperity.

My best wishes to ASSOCHAM and EY teams for Digital Financial Security Conclave 2022.

FOREWORD

Deepak Sood
Secretary General, ASSOCHAM

Cyber security has become a growing concern for banks and financial institutions, with the need to protect data from unauthorized alterations and access increasing manifold. In a race to adopt technology innovations, banks have increased their exposure to cyber incidents or attacks, thereby underlining the urgent need to implement a robust cyber security and resilience framework.

Cyber security has become a significant issue to national security in India. Most of the financial institutions and banks rely on technology for their operations. Sensitive data of banks can be at risk without proper cyber security measures taking place. Banks and other financial institutions need to know how cybercriminals operate and the latest security threats. In this context, taking all the security measures is vital to protect the data and privacy. Any breach in the security of payments is likely to affect the diligently built confidence of customers. As the government pushes for broader adoption of digital payments across multiple use cases, incidences of fraud may make customers wary of security within payment systems. Thus, it is necessary for all participants in the ecosystem to continuously make efforts to make payment security and risk management a priority for their business.

With a vast number of consumers adopting digital payments, there is a high need to discuss future-forward digital capabilities and technologies. The need of the hour is to make payments faster and safer while enhancing the user's experience, enriching decision-making for all stakeholders involved and instilling a greater sense of security for consumers. This would go a long way in designing, developing, and deploying futuristic innovations to build the country's digital economy.

I am glad ASSOCHAM is organizing the Digital Financial Security Conclave 2022. The conclave will discuss Risk & Fraud, cybersecurity, payment security, trends & innovations, the role of the network in driving security and the impact of policies, and futuristic solutions that can drive innovation in the industry and pave the path for a stronger digital economy. ASSOCHAM and EY have jointly prepared a report on Digital Financial security. The Report will help to provide more insights into the emerging challenges and solutions for the BFSI sector in data privacy and cybersecurity areas.

My best wishes to ASSOCHAM and the EY team for the success of the Digital Financial Security Conclave 2022.

FOREWORD

Ram Rakkappan
Chairman of National Council of Fintech,
ASSOCHAM

India has a significant opportunity to advance the development of its payments system and achieve important national objectives, including driving innovation and digitization, enhancing financial inclusion. Digital payments will pay a critical role in achieving the Digital India vision and in driving financial inclusion. Achieving this goal would not only help India to bring more people into the formal financial system, but also in reducing the size of the shadow economy and delivering an increase in job. However, with the penetration of digitization and the revolution it has led to in the online and digital payment, there have been increased concerns for security among the public. Cybersecurity threats are the biggest challenge to expanding digital payments.

The global payments industry is undergoing significant and rapid technological change, including mobile and other proximity and in-app payment technologies, ecommerce, tokenization, cryptocurrencies, distributed ledger and blockchain technologies, and new authentication technologies such as biometrics, 3D Secure 2.0 and dynamic cardholder verification values or dCVV2. As a result, we expect new services and technologies to continue to emerge and evolve. Technological advancements are enabling digital payment solutions providers to offer personalized experiences that are seamless and user centric. However, the same innovations are also being leveraged by malicious actors in the cyberspace to attack organizations as well as consumers to perpetrate fraud.

Today there is a greater need for industry to invest significantly in their approach to cybersecurity. The companies should deploy the security technologies to strengthen data confidentiality, integrity, and service availability, emphasizing core cybersecurity capabilities to minimize risk. Considering that India is still at an early adoption stage of its digitization journey, it is absolutely critical that the right environment for digital payments includes a comprehensive cybersecurity strategy supported by a robust framework to help all stakeholders involved in the ecosystem.

I am glad that ASSOCHAM and EY have jointly prepared a report on Digital Financial Security and will be unveiled during ASSOCHAM Digital Financial security Conclave 2022. The partnership between ASSOCHAM and EY to draft a report will help industry to take key observations, learnings, and recommendations as well as the impact of cybersecurity on various aspects of the industry. In addition to consumer best practices, key takeaways from the report include recommendations in the areas of public policy and enterprise security. Opportunities, threats, and risks in financial payment space will further emphasized to stress the importance of a holistic cybersecurity framework.

I wish ASSOCHAM Digital Financial Security 2022 event a huge success!

Thank you.

EXECUTIVE SUMMARY

The payments' function, along with its operations and technology capabilities, is the beating heart of any financial system supporting transactions processing payments for individuals, businesses, and governments.

The growth of digital payments in India has piggybacked upon demonetization and the advent of the COVID-19 pandemic. Over the last decade, the Indian payments environment has become much more dynamic, creating even greater challenges for financial institutions. Complex regulatory requirements outdated and poorly integrated legacy systems, pandemic-induced urgency and an increasingly competitive marketplace all have pushed traditional financial institutions to evaluate innovative opportunities for payments transformation. Phenomenal growth in the consumer and SME digital credit access, and mounting participation of the retail investors in the stock market are testimonials to it being one of the best digital payments ecosystems of the world in terms of value and volume[1]. However, the rising trend of digital adoption is being surmounted by the mounting charts of payment frauds such as multiple phishing, malware, fake UPI links and OTP linked frauds is making it a situation of flux.

The pressure on payments players is real, but the times are exciting. The introduction of newer and quirkier payment methods, industry collaborations, tech advancements and regulatory support are making space for a lot of innovation and best practices in two important customer agendas - security and convenience. Winners shall be the ones who are quicker in finding the delicate balance between the two.

Rise in cybercrime is a menace to the global economy, leading to pernicious effects on businesses and communities. Disruptions in the processing of payment flows is additional threat to the payment systems. As organizations innovate and undergo digital transformation, it is imperative for them to have a robust and scalable payment infrastructure.

But, with a strong regulatory focus and multiple governmental headways into it, payment players have tides flowing in their favor. Some of these critical drivers include:

- Adoption of ISO22022 Standard: To increase interoperability among local and international financial institutions. It uses an XML format which allows context-specific payment information to be specified, resulting in high quality of data.
- Adoption of PCI DSS 4.0: Developed with a zero-trust philosophy, allowing firms to create their own distinctive, pluggable authentication systems to satisfy the legal requirements for data protection.
- Introduction of RBI's Digital lending guidelines: Leading to an increase in adoption by Micro, Small & Medium Enterprises (MSMEs). Online lending platforms have gained massive popularity among MSMEs post the pandemic as they could not secure finance through traditional lending institutions and thus had to switch to digital loans.
- Security layer of tokenization: Credit and debit card tokenization is the procedure of substituting sensitive data with a token, which is randomly generated, one-of-a-kind placeholder, known as a 'token'.
- Proposed use of Data Localization: Data localization may improve India's governance of payment-related data significantly and is focused on protecting the customer's interests and data.

Government of India's take on the personal data protection bill: The Government of India has released a draft of the Digital Personal Data Protection Bill for public consultation in November 2022. The bill is applicable to processing of digital personal data within the territory of India collected online or collected offline and later digitized. The growth of Indian payment security is driven by a bunch of nurturing initiatives undertaken by the government and regulators for a buoyed funding environment. These aim to offer an ecosystem that is geared up for strengthening the security and compliance design, enhance enterprise security, and proactively monitor and predict fraud monitoring. Organizations, on the other hand, need to play their role as well and invest in effective security measures to enhance growth and underpin their trust in the system.

Kartik Shinde
Partner and Financial Services
Cyber Security Leader, EY LLP

Kartik.Shinde@in.ey.com

Ranadurjay Talukdar
Partner and Leader, Payments, EY LLP

Ranadurjay.Talukdar@in.ey.com

1. Total 8 bn digital transaction volume of INR 3,021 lakh cr recorded in FY 2022

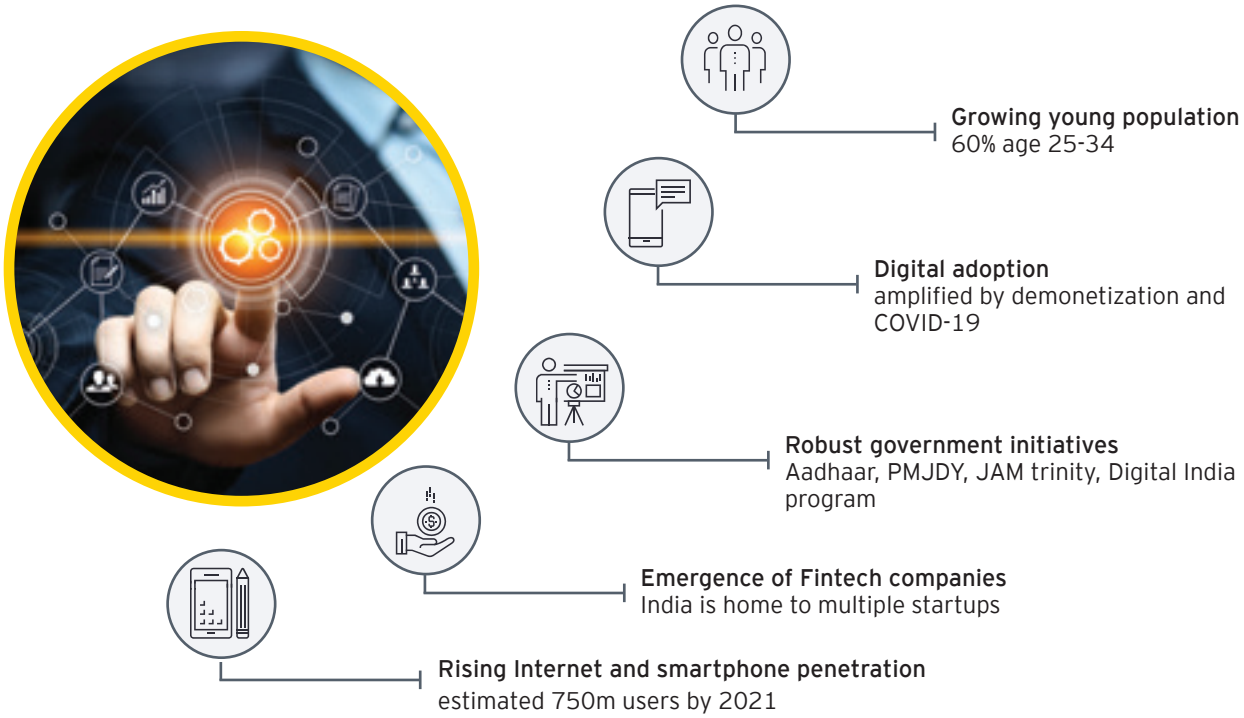
01

The fast-changing facets of payments landscape in India

The payments market in India is in a swift flux situation owing to the introduction of newer and quirkier payment methods, industry collaborations, tech advancements and regulatory support. Overall, the sector has undergone a rapid transformation from the otherwise traditional patterns where banks played the role of facilitator amid merchants and customers. The challenger newbies in the industry have long turned down the skepticism with which they were looked at when they first made their mark. They have come far from challenging and contradicting the archaic beliefs that bricks-and-mortar branches enthused trust garnered over years.

With technology advancing and customers scouting for a seamless experience across multiple channels, payment companies have moved the needle to hold a much predominant role. Payments is no more just a mode of facilitating the transfer of funds. It is now targeting a larger role of redefining the customer experience and offering ease of use to customers and merchants.

1.1 The propellers of India's digital revolution



Rising consumer appetite for digital payments powering the spread of payments-focused FinTech companies.

The financial inclusion index (tracks financial services extended to unbanked) recorded a growth of 4.6% in March 2022 on a YoY basis[2]

Market dynamics are forcing the incumbents in this space, including banks, FinTech companies and payment processors to invest heavily in payments modernization.. Many of them are eyeing collaborating with established as well as niche players to cater to the evolving stakeholder preferences. Big tech companies have ventured into the space and customers have demonstrated a likeness to this combination of technology and banking as it saves them time and money. Challenging the status quo with traditional finance companies, this fusion of big-tech and banking seems to have reached mass adoption.

2. RBI; The financial inclusion index (tracks financial services extended to unbanked) was 56.4 in March 2022 in comparison to 53.9 in March 2021; the same was 43.4 in March 2017; https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=54133

1.2

Traditional + emerging = Multiple avenues available to pay

Consumers are spoiled with choice and are eyeing cashback and rewards as a motivation to choose one over another.

The organizations are giving in to rapidly changing customer dynamics, where customer centricity has paved way for customer obsession. It has become imperative for organizations to offer multiple avenues to pay to be able to hold the customer. Offering a plethora of choice in payment methods, including traditional modes of net banking, debit, and credit cards etc. to the newer versions of BuyNow Pay Later, mobile wallets, there is a strategic link back to offering a better checkout experience to the customers. In fact, many customers agree that they defer their purchase and sometime even cancel it if their preferred payment method is not offered as a choice. FinTech companies are playing an important role in increasing the banked population around the world. In India, UPI remains the biggest success story (7.3billion transactions in October 2022[3]), with an all-time highest number of transactions since its launch six years ago).

Rapid adoption of technology and innovation, supports not only the growth in digital payments but also the availability of a safe, secure, innovative, and efficient payment ecosystem.

Digital payments in India have seen widespread adoption - 216% growth in total digital payments volume in March 2022 as compared to March 2019.

Digital payments have become a critical enabler of e-commerce sales, supporting the expansion of businesses small and large to new customer segments and even new global markets.

3. https://www.npci.org.in/statistics/monthly-matrix

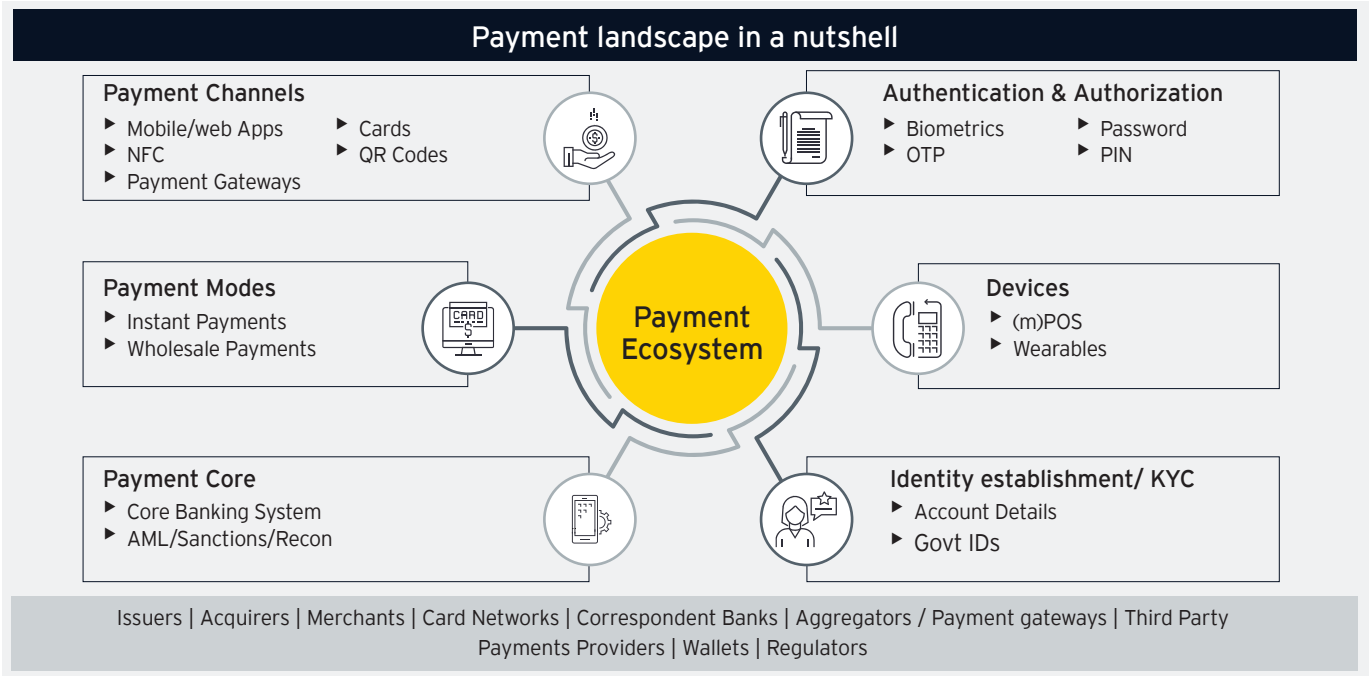
1.3

The orchestration of a payment ecosystem

From product's production to consumer's consumption and every payment in between

It takes multiple parties to perform a single successful payment. In its most rudimentary form, the payment streams from the payer's financial institution to the payee's financial institution via some type of rails or grid. The stream that ties the two financial systems is fundamentally the synchronization of the payments system, and there are multiple categories of networks, including central banks and network providers.

The involvement of multiple players or touchpoints in a transaction flow and possible gaps within their respective networks exposes the ecosystem to the risk of fraudsters sweeping in. Besides, there are payment challenges, such as the need for currencies to be exchanged through incongruent financial systems, and taxation and safety procedures. Fraudsters are devising newer mechanisms and adopting the latest technologies too to dupe the users through social engineering methods or at times, loopholes in the infrastructure.



The boon in the bane demands players to fight the odds together

According to a recent survey by EY in September 2022, 44% of Indian consumers transact with FinTech companies and digital banks and more than 63% feel comfortable managing their finances using a virtual assistant. Of the total group surveyed, 60% belong to the age group of 25 to 34 comprising GenZ and millennials who would form the majority of customer base in the coming years. While these are encouraging numbers, one cannot ignore the fact that the mounting digital adoption is also giving rise to resultant frauds. Fraudsters are on a spree in devising newer ways of challenging the consumer vulnerabilities.

Many are falling prey by sharing sensitive information and losing their money. Contactless payments have paved the way for multiple phishing, malware, fake UPI links and OTP linked frauds.

The scenario makes it imperative for the incumbents to devise mechanisms, keeping in mind customer's safety and transaction security

> Rapid digital adoption opening a myriad of doors for fraudsters who are looking for loopholes

02

Frauds and Risk Management in Digital payments

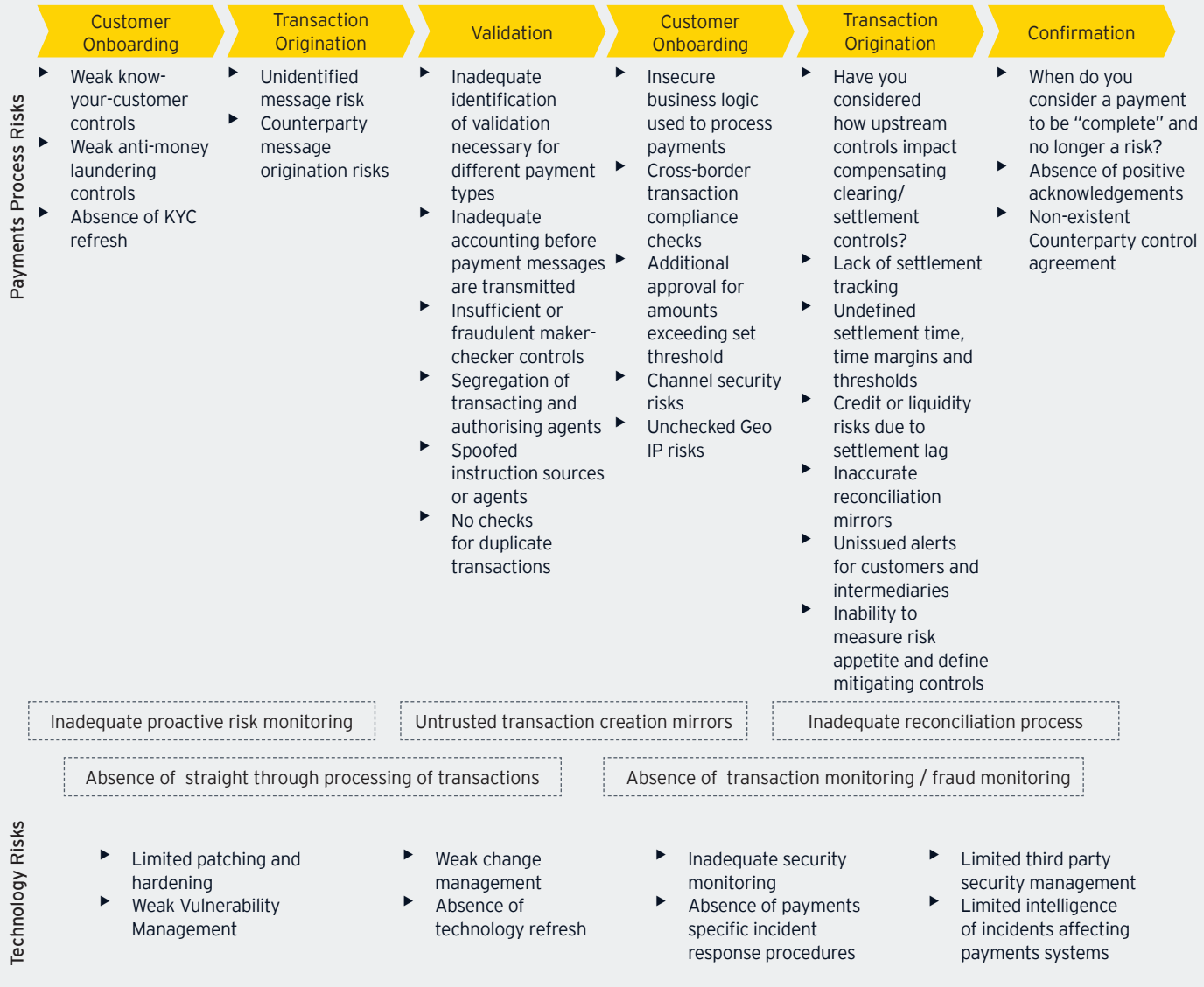
The increase in adoption of digital payments is also seeing a rise in targeted cybercrimes and further sophistication in the types of attacks

With an increase in adoption of digital payments, ecosystem partners are juggling to create a delicate balance between convenience and security. The payment transaction value chain is now facing more threats than ever before. The risks can be broadly classified into two categories – targeted cybercrime and fraud and disruptions in the payment flows.

The image below depicts current risks that are being exploited by fraudsters across the payment lifecycle. There is an increased need for organizations to work together synchronously to reduce the cascading impact of these risks.

Keys Risks in Payments Lifecycle

A firm grasp on the payments life cycle, including points of failure and areas prone to attack, and key payment risks and controls is critical in preventing / detecting a payments fraud. The below are the key risks that need to be addressed throughout a payments lifecycle.



2.1

Cyber Crime and Fraud

Cybercrime and fraud are considered prominent threats to the payment technology owing to their rapid spread. In a complex, ever-changing world, financial cybercrime risks proliferate as one of the largest systemic risks to the global economy, often yielding devastating impacts on businesses and communities.

As financial services organizations struggle to proactively secure the systems, the threat of cyber fraud continues and there is an increasing need for change and innovation. Technology has created a host of new pathways for criminal gangs to launder the proceeds of their illegal activity and gain money out of it. As consumers continue to migrate to digital channels, many organizations are still struggling to detect and prevent fraud.

The following are some of the more recent methods used by fraudsters to commit a cybercrime or fraud in the payment ecosystem:

Synthetic identities:

It is one of the fastest growing online crimes - combines elements of real and falsified information and a multimillion-dollar problem owing to growing online banking and digital financial services. The fraudsters here use a combination of personally identifiable information (PII) to fabricate a person or entity along with photographs, date of birth available on the social media platform. It is also one of the most difficult types of identity fraud to detect due to a lack of any real person to report the fraud. While Aadhaar based KYC reduces this risk significantly in India, but globally this is a very prevalent risk and is used to enable to money mule network.

ATO Fraud & APP Fraud via Social Engineering:

Armed with personal credentials obtained through the dark web or phishing or even social media, fraudsters launch account takeover (ATO) and compromise the legitimacy of a user's account. The method puts to use social engineering to dupe victims by authorized push payment (APP) tactics.

Authorized push payment (APP) fraud, also known as APP fraud, is used by fraudsters to deceive consumers or individuals at a business by manipulating them to send a payment under false pretenses to a bank account controlled by the fraudster. Such payments are made using real-time payment schemes and therefore cannot be revoked.

While frauds related to synthetic identities is relatively less common in India compared to some of the western countries. Aadhaar linked authentication along with virtual on-boarding during the pandemic has led to an increase in such frauds in India as well.

2.2

Disruption in the processing of payment flows

Disruption in the processing of payment flows is another key threat to the payment systems. As organizations are going through a significant digital transformation, it is necessary for them to have a resilient and scalable payment infrastructure. The payment flows can disrupt due to a plethora of reasons like server downtime, expired certificates, connection interruption between applications, invalid inputs, misconfiguration, delayed transaction authentication, etc. The sheer complexity of the architectures often makes it difficult to trace the issue resulting in the disruption.

The payment systems have their unique set of threats that exploit the weaknesses in it and expose the systems to various risks associated with it. The commonly found vulnerabilities in the payments systems are described below:

Vulnerabilities in payment infrastructure

Exploited to perform attacks like:

- price manipulation
- overflow for shopping carts
- intercepting transaction data capturing
- intra-bank network payments

Breach of transaction and customer data

- Assorted attempts of intellectual property or classified information
- Impact of this information being sold on dark web is not limited to organizations but also affects its consumers

Limited regulatory compliance

Despite increased focus on cybersecurity by regulatory bodies, implementation deadlines are extended due to a lack of adaptability in compliance requirements

Insecure payment architecture

If the payment architecture is insecure, the stakes and possibility of breaches are high, thereby reducing customer trust on digital payments.

The ecosystem vulnerabilities can risk the businesses with financial loss, cyber espionage, regulatory impact, as well as reputation loss. Financial services organizations around the world are under greater scrutiny over their conduct and cyber security related risks, making them dive deeper into the need for protecting the interest of the customer and stakeholders alike.

Many organizations are fighting an uphill battle when it comes to detecting and preventing fraud. Consumers continue to migrate to digital channels, and while this transition benefits organizations, it comes at a cost. The pandemic's effects have expedited the digitization of customer interactions by several years. Customers are becoming more comfortable and confident in consuming these services online as businesses continue to move their services into the digital space. Although digital transformation was already on the rise prior to the pandemic, it took on new urgency once the corona virus struck. The pandemic fundamentally altered how people interact with businesses, opening a new pool of inexperienced digital users for fraudsters to prey on.

Businesses are constantly trying to strike the right balance of opportunity and risk. Balancing fraud and customer friction across multiple channels is even more difficult (e.g., mobile, web, point-of-sale). A mismatch between authentication methods and transaction risk can lead to friction in the customer journey, leading to lower conversions. To further reduce fraud and provide the right level of conflict, merchants and issuers are looking for alternative authentication solutions to maximize customer experience and minimize unnecessary collisions. required during the referral and payment process.

> Although each additional piece of personal information provided by consumers can help to reduce fraud, it also adds friction to the user journey, which can lead to a transaction getting abandoned.

03

Minding the gap through planned initiatives

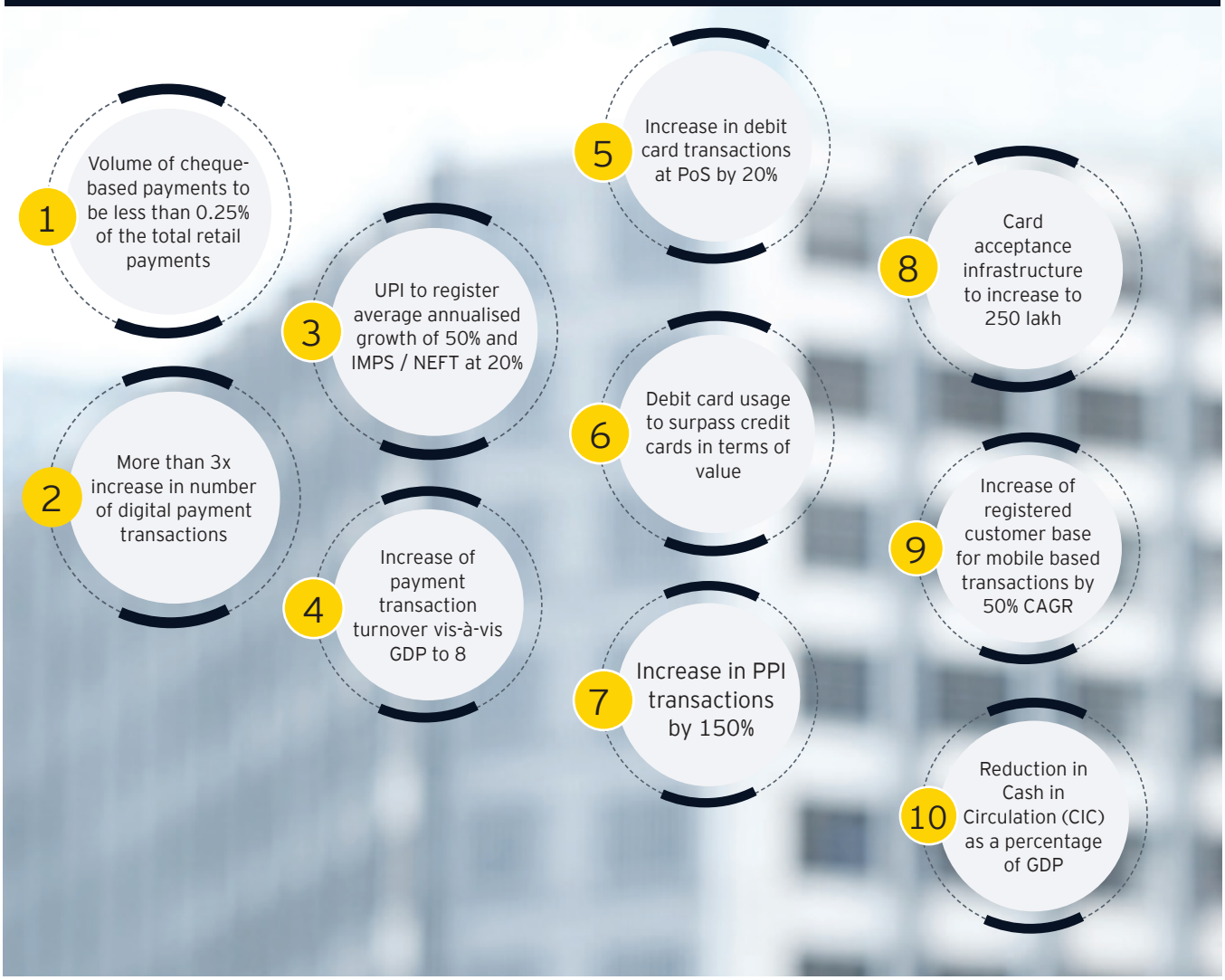
Managing the thin line of security between secure and easy to use

Next generation payments methods are spearheading the rising tides in digital payments adoption. Leveling up from customer centricity to customer adoption, this race to offer umpteen convenience to customers is driving the new era of payments. The India story of digital ID infrastructure powered by UPI, JAM trinity has been substantial in driving the mass adoption and making payments more transparent. The FinTech players, powered by the emergence of big tech, are agile and offer seamless direct-to-consumer (D2C services, empowering customers on the way. Besides, the operational advantages of open ecosystems are fueling the growth with more and more banks strategically investing in them.

Additionally, there is an increased scrutiny from the Indian regulators across the payments ecosystem on transaction service participants demanding a higher level of accountability and traceability.

RBI's Payment Vision 2025 released in June this year is a further step in the direction. The document outlines key focus areas that could impact the industry over the next few years.

RBI Payment Vision 2025 Goals



Besides RBI'S Payment Vision 2025, mentioned here are some of the initiatives pinned by the regulators to offer a levelled playing field for the incumbents in payments and financial services industry in general

3.1 Adoption of ISO22022 Standard

A common international standard for financial messaging, which is structured, data-rich, and offers standard rules

Processing of high-value cross-border transactions has been a challenge across the industry. This is mainly due to the lack of common formats and standards across borders. Hence, the world is now moving towards ISO 20022 to increase interoperability among local and international financial institutions. It uses an XML format which allows context-specific payment information to be specified, resulting in high quality of data.

It may result in better straight-through-processing (STP) rates and automatic reconciliation processes, increased payment speeds and reduced costs. A seamless global payments system results in reduced manual efforts and translations, allowing banks and financial institutions to pursue value-added data-driven services, thereby offering better customer experience.

Globally, 70+ countries are already using ISO 20022 in their domestic payment systems, including Switzerland, Japan, China and India.

According to the timelines given by SWIFT, banks across the globe need to update their messaging infrastructure ahead of November 2022. Since migration to ISO 20022 is a complex process, and organizations may be at different stages of readiness, SWIFT has specified a global rollout timeline from November 2022 - November 2025, where the legacy SWIFT MT messaging and ISO 20022 will continue to co-exist. Federal Reserve has proposed adoption of ISO messaging standard by end of the year 2023.

To achieve strategic transformation, organizations must assess their current state, and do an impact study of the changes that affect the payments value chain. To do so, organizations would need to:

- Consider ongoing initiatives that overlap with ISO 20022
- Identify the impact of ISO 20022
- List gaps with respect to operations, applications, infrastructure, integration
- Develop a strategic transformation plan
- Identify vendors and partners to close the gaps
- Develop a roadmap and a migration plan.

3.2 Adoption of PCI DSS 4.0

The PCI DSS 4.0 standard is developed with a zero-trust philosophy, allowing firms to create their own distinctive, pluggable authentication systems to satisfy the legal requirements for data protection. Although a 'zero trust' model is not directly mentioned in the new standard, it is clear the PCI Security Standards Council is moving in that direction. Looking at how the standards are different in PCI 4.0, we see a trend. There is a subtle shift away from precise technical specifications and towards a broader view of security. The standard demands stronger authentication methods, advanced encryption methodologies, and has also brought out the customized approach concept with the goal of addressing the emerging threats and allowing organizations the flexibility to come up with unique ways to combat new threats to payment information.

PCI DSS v 4.0 has already been released by Payments Council and payment ecosystem participants have been provided a transition period until 31 March 2024 to adopt the standard.

3.3 RBI digital lending guidelines

India's digital lending market has grown quickly and facilitated $2.2 billion in digital loans in 2021-22, with startups attracting foreign backers and giving traditional banks a run for their money in the credit business.

Digital lending is mostly preferred by those who generally cannot avail any credit through formal sources of finance like banks. One of the prime examples is the increase in adoption by Micro, Small & Medium Enterprises (MSMEs). Online lending platforms have gained massive popularity among MSMEs post-COVID-19 as they could not secure finance through traditional lending institutions and thus had to switch to digital loans. Based on the Digital Lending guidelines released this year, organizations will need to primarily focus on the following from a technology and data standpoint:

- Developing a **comprehensive website privacy policy** including details of third parties that are allowed to collect personal information
- Collection, usage and sharing of data with third parties based on the principles of **data minimization, consent and purpose limitation**. Periodic due diligence of such third parties should be enforced
- Increased responsibility on Regulated Entities (REs) to ensure **privacy and secure storage of data**
- Regulated entities will need to ensure that **Lending Service Providers (LSPs) engaged by them comply with various technology standards** as per regulatory requirements

3.4

Laying down a layer of security through tokenization

The quick transition to digital transactions or online payment entails the need for convenience, security, and dependability. Tokenization is, therefore, a crucial step in this direction because it provides protection against data breaches and serves as a protective layer in the digitized payment ecosystem by encrypting card information and protecting both consumers and merchants from cyberattacks. With the inclusion of Card on File Tokenization (CoFT) and incremental changes in regulatory compliance requirements, the industry has faced challenges in implementation. The additional onus of ensuring ecosystem compliance placed on the Card Payment Networks (CPNs) by the regulators has led to an increase in oversight of the CPNs on entities traditionally considered as customers and / or service recipients.

3.5

The underestimated power of data localization

While the directive set by the RBI regarding data localization may improve India's governance of payment-related data significantly and is focused on protecting the customer's interests and data, some parts of the financial services industry are still struggling to demonstrate compliance against the regulation even after close to five years of the initial directive. Most organizations have adopted large-scale technology migrations, leading to an increase in the application and infrastructure landscape present in India. Ongoing governance and sustenance of the set-up in India would be an area of focus for auditors and regulators alike.

3.6

Putting the foot down with our own data privacy bill

The Government of India has released a draft of the Digital Personal Data Protection Bill for public consultation in November 2022. The bill is applicable to processing of digital personal data within the territory of India collected online or collected offline and later digitized.

It is also applicable to processing made outside India if it involves profiling of or providing goods or services to the data principles within the territory of India. The proposed bill exempts certain entities from various compliances, including sharing details for data collection purposes. These entities are notified as data fiduciaries. They are exempted from provisions which deal with informing individuals about the purpose of data collection, collection of data of children, appointment of data auditor, risk assessment of public order, etc.

Regulator driven scrutiny measures are few critical steps in the right direction. Further the gaining momentum of technological advances are expected to pave way for a future where payments are tightly secured and gaps zipped

04

Security as an enabler to widen digital payments adoption

Increase in the sophistication of cyber-attacks makes it imperative for institutions to consider security as a business enabler rather than a trade-off

Digital payment's long-term success is dependent on a robust regulatory framework that is:

- easy to use and convenient
- offers an active customer redressal framework
- proof-checked on security measures to aid confidence and trust
- incentivizes higher contribution and benefits in comparison to cash transactions

Many players are already thinking on the lines of investing and implementing security features to eradicate payment threats related to cybercrime, account takeover, social engineering. Financial service providers are working with vendors and third parties to promote service and security that must be used in a coordinated approach to create an innovative offering, which includes the elements of trust and customer convenience in the overall experience design.
It will be imperative for them to design use cases with ideal transaction flows and data exchange to streamline payment transactions. Likewise, while processes around data privacy and information security are indispensable, it is crucial to realize the trade-off with customer convenience.

4.1

Security and compliance by design

One way of improving the security of payment systems is to implement security throughout the product lifecycle. This includes a close integration of stakeholders from business, technology, security and compliance teams, enabling a more secure by design product. Embedding security and regulatory compliance requirements in the lifecycle would reduce efforts / costs associated with enhancement and modifications at a later stage. Such products are also known to be more resilient since they have been reviewed by stakeholders across teams with a wider variety of test cases.

Solving security issues at the beginning is much cheaper, by a factor of 100, according to research. On top of that, the pressure of time and budget constraints is particularly heavy at the end of the development process, not the best time for thought-out improvements. Security by design results in a more resilient system where security is built in rather than hastily added as a fix.

Implementing a variety of measures in security by design (awareness, knowledge, tools, and checks) allows security flaws to be removed more effectively than by testing at the end of development.

Determining exactly which errors have been made allows you to adapt the development process to prevent further errors. This applies, for example, to improvements in the collaboration between developers and the IT operation. Close and automated collaborations are referred to as DevOps; or SecDevOps with security built in.

4.2

Ongoing enhancement of enterprise security and resilience

Organizations must continue to focus on periodic security testing, threat hunting and red teaming activities to proactively review their security posture. Resilience of critical applications in the payment chain should be tested in a collaborative manner to avoid cascading impacts due to failures in individual organizations. It is imperative that the industry enables the creation of a secure ecosystem that would lead to both optimization as well as value creation across the payment chain.

4.3

Proactive monitoring and predictive fraud monitoring

Proactive monitoring has been around for a while, but it has recently gained popularity owing to the rising traction of managed IT services. Proactive monitoring is a technique used for detecting potential problems before they disrupt operations in the context of cybersecurity. Most of the time, businesses do not adequately prepare for potential cyber incidents until it is too late.

Proactive cybersecurity refers to everything you do before an attack occurs. This is where new age technology platforms play an integral role by leveraging analytics and advanced fraud behavior modeling. Computing risk scores for transactions in real-time and enables payment service providers to identify potential frauds to get an increased rate of accuracy in fraud detection. Researchers have also started exploring the possibility of quantum computing by developing algorithms for fraud detection that could be faster and more accurate than algorithms in use today.

Now is a pivotal time for the organizations to assess the level of innovation in security across the payments landscape for enhancing trust and business advancement. There is a significant opportunity to transform payment security offerings to deliver better customer experiences, simplify back-end infrastructure to keep up with the pace of change, regulatory guidelines and leverage innovations to benefit both business and consumers- all while maintaining the security and stability that underpins trust.

05

Key recommendations

Security moved beyond the server room to step into the board room

Key suggestions for the industry to up their game in maintaining security and driving customer confidence

With the growing number of channels for digital payments and the anticipated exponential rise in customer adoption of these products, the challenge of securing them will only continue to get more complex. The diversity in security maturity across the ecosystem participants only compounds the issue. Real-time payments need real-time security and enhanced fraud detection abilities for organizations. Following are some key areas that organizations across the board must prioritize as a part of their business strategies.

1 Proactive testing of cyber maturity

- Test cyber-attack detection and defense controls
- Conduct compromise assessments
- Perform periodic threat modeling to identify and manage current risks

2 Security, privacy and compliance by design

- Ensure products and processes consider security, privacy and compliance requirements throughout the lifecycle
- Drive engagement of information security architects during product ideation
- Enable a cultural shift within the organization by adopting strong design principles for security, privacy and compliance

3 Advanced incident and fraud detection

- Implement proactive fraud and incident detection solutions based on behavioral analytics
- Develop or keep forensic capabilities on standby
- Conduct simulation activities / drills periodically, including Board and Senior Executives

4 Enhance stakeholder awareness

- Have effective communication and engagement with customers
- Create an ecosystem for knowledge sharing regarding cyber incidents / frauds across the ecosystem
- Mandate awareness trainings for employees based on their job roles
- Upskill security teams to manage changes in technology and the business landscape

5 Drive ecosystem security

- Develop security baselines for all participants in the payments chain
- Implement controls to manage risks associated with service providers

Our offices

Ahmedabad
22nd Floor, B Wing, Privilon
Ambli BRT Road, Behind Iskcon
Temple, Off SG Highway
Ahmedabad - 380 059
Tel: + 91 79 6608 3800

Bengaluru
12th & 13th floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground Floor, 'A' wing
Divyasree Chambers
11, Langford Gardens
Bengaluru - 560 025
Tel: + 91 80 6727 5000

Chandigarh
Elante offices, Unit No. B-613 & 614
6th Floor, Plot No- 178-178A
Industrial & Business Park, Phase-I
Chandigarh - 160 002
Tel: + 91 172 6717800

Chennai
Tidel Park, 6th & 7th Floor
A Block, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100

Delhi NCR
Golf View Corporate Tower B
Sector 42, Sector Road
Gurugram - 122 002
Tel: + 91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Gautam Budh Nagar, U.P.
Noida - 201 304
Tel: + 91 120 671 7000

Hyderabad
THE SKYVIEW 10
18th Floor, "SOUTH LOBBY"
Survey No 83/1, Raidurgam
Hyderabad - 500 032
Tel: + 91 40 6736 2000

Jamshedpur
1st Floor, Shantiniketan Building
Holding No. 1, SB Shop Area
Bistupur, Jamshedpur – 831 001
Tel: + 91 657 663 1000

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 433 4000

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

Pune
C-401, 4th floor
Panchshil Tech Park, Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

Ernst & Young LLP

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C,
Kolkata - 700016

ED None
EYIN2212-013

RG

Contributors

- Shruti Bajpai
- Parag Sanghvi
- Ritu Arora
- Aniket Bhosle
- Manasi N J

ey.com/en_in

@EY_India EY EY India EY Careers India @ey_indiacareers

About ASSOCHAM

The Associated Chambers of Commerce & Industry of India (ASSOCHAM) is the country's oldest apex chamber. It brings in actionable insights to strengthen the Indian ecosystem, leveraging its network of more than 4,50,000 members, of which MSMEs represent a large segment. With a strong presence in states, and key cities globally, ASSOCHAM also has more than 400 associations, federations and regional chambers in its fold.

Aligned with the vision of creating a New India, ASSOCHAM works as a conduit between the industry and the government. The Chamber is an agile and forward-looking institution, leading various initiatives to enhance the global competitiveness of the Indian industry, while strengthening the domestic ecosystem.

With more than 100 national and regional sector councils, ASSOCHAM is an impactful representative of the Indian industry. These Councils are led by well-known industry leaders, academicians, economists and independent professionals. The Chamber focuses on aligning critical needs and interests of the industry with the growth aspirations of the nation.

ASSOCHAM is driving four strategic priorities – sustainability, empowerment, entrepreneurship and digitization. The Chamber believes that affirmative action in these areas would help drive an inclusive and sustainable socio-economic growth for the country.

ASSOCHAM is working hand in hand with the government, regulators, and national and international think tanks to contribute to the policy making process and share vital feedback on implementation of decisions of far-reaching consequences. In line with its focus on being future-ready, the Chamber is building a strong network of knowledge architects. Thus, ASSOCHAM is all set to redefine the dynamics of growth and development in the technology-driven 'Knowledge-Based Economy. The Chamber aims to empower stakeholders in the Indian economy by inculcating knowledge that will be the catalyst of growth in the dynamic global environment.

The Chamber also supports civil society through citizenship programs, to drive inclusive development. ASSOCHAM's member network leads initiatives in various segments such as empowerment, healthcare, education and skilling, hygiene, affirmative action, road safety, livelihood, life skills, sustainability, to name a few.

Deepak Sood

Secretary General
ASSOCHAM
sg@assocham.com

The Associated Chambers of Commerce and Industry of India (ASSOCHAM)
4th Floor, YMCA Cultural Centre and Library Building,
01 Jai Singh Road, New Delhi – 110001
Website: www.assocham.org