The digital payments ecosystem of India: Planning security today for a resilient tomorrow

March 2025

The better the question. The better the answer.
The better the world works.

Shape the future
with confidence

Table of contents

Foreword

Murali Rao

Partner and Cybersecurity Leader,
EY India

The wave of digital payments adoption in the country is so big that the security of the digital payments ecosystem is a matter of national importance both in terms of the potential impact on the economy as well as building trust among people while realizing the “Digital India” dream.

As the payments ecosystem continues to evolve and grow rapidly, organizations in this space have a marked advantage in terms of adoption of new-age technologies and can become trendsetters in the field of cybersecurity.

While cyber-attackers are gaining easy access to increasingly sophisticated tools which are not only intuitive but also faster than before, most cyber security incidents in the payments ecosystem reveal that fundamental security flaws are being targeted even today. A collaborative approach across the ecosystem in threat and fraud monitoring will enable a stronger proactive approach to threat identification. Although it may not be easy to stay ahead of the attackers, the key measures of success will be how fast one can predict and detect a cyber-attack and how resilient the payments product is in the face of one. The question is no longer ‘If there will be an attack’, it is ‘when there is an attack, how soon can we recover’.

As we delve into the nuances on payments security and resilience through this knowledge document, we share our perspective on recent trends and our experiences with the aim to create a thought process towards building a more secure digital payments ecosystem. We truly believe that the digital payments ecosystem in the country is being adopted as a success story globally and it is a collective responsibility to build integrated security strategies and address payments product risks on priority.

Foreword

Ranadurjay Talukdar

Partner and Payments Leader,
EY India

As India continues to march ahead in the era of digital payments adoption, cybersecurity and resilience are key pillars that act as business drivers to enhance customer trust. The digital payments ecosystem has been in a flux over the past decade, with traditional payments participants innovating their products with a focus on customer centricity and experience, as well as new entities entering the digital payments space and experimenting with products and technology in various ways. This evolution has not only led to rapid technological transformation in the ecosystem but also helped revisit legacy security architecture to enhance and address current security strategies. The next wave of digital payments adoption will rely on resilience of the payments ecosystem and the customer's trust in new digital payments products. It is, therefore, a collective responsibility of the ecosystem to collaborate, innovate, and safeguard consumer interests.

Payments fraud management is another aspect that needs dedicated attention. While card related fraud management frameworks have evolved, considerable progress is required in addressing use cases related to Real Time Payments (RTP) fraud use cases. Increase in incidents of fraud makes the consumer vulnerable and could lead to a trust deficit. A lot remains to be done in enhancing consumer protection measures in payments frauds in India.

While the country continues to take the India payments stack and products global by setting product and feature benchmarks, it is also essential that the ecosystem builds products that are secure and compliant by design, while continuing to keep the customer at the center. At the same time, it is also important for security service providers to build lean solutions that new-age technology adopters and digital native organizations can use. There is a huge opportunity for the industry to collaborate, as has been done globally via SWIFT's Customer Security Programme (CSP) framework or the US Federal Reserve's FraudClassifier Model, that will allow superior fraud detection without impacting payment success rates.

Through this document, we aim to highlight critical aspects that would contribute to a stronger and more resilient digital payments ecosystem by sharing our perspective and experience based on a combination of technical specialization in the field of cybersecurity along with a holistic understanding of the digital payments ecosystem in the country. Together, we look forward to shaping the future of payments in the country with confidence.

Executive Summary

India's digital transformation has propelled the nation into a new era where payments are not just a transaction but also a dynamic blend of technology, innovation, and security. With the Department of Financial Services within the Ministry of Finance actively driving the promotion of digital payments in the country, the sector has seen a compounded annual growth rate (CAGR) of 44% in FY 2023-24 and which is expected to continue to grow even in the current financial year[1]. In the Banking, Financial Services, and Insurance (BFSI) sector, over 95% of banking payment transactions are now digital and digital platforms are expanding 30% annually[2].

While the digital payments ecosystem has evolved significantly over the last few years with fintech companies championing the use of new-age technology, changes in the cyber threat landscape has impacted entities small and large alike. Recent incidents highlight how attacks on supply chains can impact multiple entities within the payments ecosystem, leading to a pernicious effect on businesses, consumers, and the country's economy at large. Systemic risks need to be addressed without delay and a collaborative approach to address cyber and fraud risks is essential.

As entities continue to adopt a compliance driven security approach, it is imperative that security strategies and budgets consider adoption of security solutions and technologies to combat the current threats to digital payments flow. Adoption of Generative AI- and AI/ML-based security solutions can enable organizations in predictive threat and fraud detection and response.

Through this knowledge compilation we attempt to share our perspective on the current opportunities, challenges, and trends in the payments ecosystem in the country. By supporting solutions to the challenges of today and preparing for the problems of tomorrow, we are 'All In' to contribute towards building a more secure and resilient digital payments ecosystem in India.

Kartik Shinde

Partner, Cybersecurity Consulting,
EY India

Aniket Bhosle

Partner, Technology Consulting,
EY India

[1] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2057013#:~:text=Digital%20payments%20in%20India%20have,(CAGR)%20of%2044%25.

[2] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2098487#:~:text=India%27s%20digital%20economy%20contributed%2011.74,and%20employed%2014.67%20million%20workers

The current state of digital payments in India: Ubiquitous and frictionless

The India we live in today has adopted digital payments in more ways than one would have anticipated a decade ago. While UPI has become synonymous with digital payments, India has a wide variety in digital payments instruments for consumers and businesses. The ease of use has enabled adoption and contributed towards enhanced financial inclusion over the last decade.

India is recognized as a pioneer in Real Time Payments (RTP) products globally. As per ACI Worldwide Report 2024, approximately 49% of the global RTP transactions in 2023 were in India and approximately 70% of digital transactions have been through UPI. This is not only an indicator of the popularity of the product but also supports the reason why other countries have started adopting and leveraging the 'India stack' while building their own RTP products.

Based on the increasing digital payments footprint – from 2,070 crore transactions in FY17-18 to 21,519 crore transactions in FY24-25[3]– the entire payments ecosystem in India is witnessing an influx of varied entrants. From small start-ups to large conglomerates and entities from non-financial services backgrounds such as transit operators and transport providers have entered this space. Recent data highlights a higher growth in adoption of contactless and RTP products compared to traditional payments channels. The total number of UPI transactions grew by 57% year-on-year, from 8,324 crore transactions in FY23 to 13,096 crore transactions in FY24[4]. There has also been an increase in transaction values on UPI and other digital payments channels. Both these trends indicate an increasing customer trust in the digital payments ecosystem.

However, along with the successful adoption of UPI as an instrument of choice, the unfortunate reality is that fraudsters have leveraged the product to their advantage as well. UPI fraud cases surged 85% in FY24. The number of incidents rose from 7.25 lakh in FY23 to 13.42 lakh in FY24[5]. These cases involved a total value of INR1,087 crore, compared to INR573 crore in the previous year. Other digital payments instruments have also seen an increase in fraud. As per RBI's report on Operations and Performance of Commercial Banks dated 26 December 2024, the share of internet and card frauds in total stood at 44.7% in terms of amount (225 crore out of 1,146 crore) and 85.3% in terms of number of cases (7,454 cases of 8,919 cases reported) for the period April to September 2024[6]. The frequency and rate in increase of such frauds has led to skepticism regarding security measures across the ecosystem. Payments product strategies are evolving to add elements of friction in the customer journey to tackle fraud risks. Managing customer experience and safeguarding customers from such risks is truly a balancing act.

Recent incidents of unplanned outages and unavailability of systems facilitating payments have also raised concerns as India continues to progress towards a less-cash economy. In 2024, on an average, 14 banks were impacted multiple times in a month, leading to unplanned outages of an average 143 hours a month in their UPI products[7]. Hence, questions arise on whether banks, fintechs and other ecosystem participants have anticipated the volumes of transactions and planned capacity and resilience requirements adequately. Another risk related to concentration is when a single entity that provides services to multiple payments participants is impacted. Case in point being the supply chain incident at a major technology service provider that impacted the payments service interface with National Payments Corporation of India (NPCI) in July 2024. While the monthly transaction volume on UPI was noted to grow at an average of approximately 3% in 2024[8], it slowed for a couple of months following the incident.

Such incidents have prompted focused regulatory action, communicated through advisories, guidelines, and during inspections as well. The punitive approach adopted by the regulator across the payments ecosystem in the last 5 years due to observed non-compliances has created ripples across the payments ecosystem in India as well as globally.

The regulators have also planned and implemented multiple initiatives to secure the payments ecosystem. Requirements to have a secure and resilient payment product have been mandated right from the point when an entity initiates the license application process and continue post license issuance also through reviews and inspection of baseline security controls. Hence, while the size and scale of the payments participants varies, the minimum security controls mandated provide a guardrail to safeguard the ecosystem.

The innovative initiatives by the regulator are noteworthy, specially through the adoption of emerging technologies such as identification of mule accounts using the in-house developed AI/ML platform[9] and providing platforms to payments participants for centralized fraud monitoring and reporting.

Regulators are being recognized as the pivotal architects of a safe, secure, reliable, accessible, affordable, and efficient payments landscape (the key pillars of Payments 2025 vision). In a market driven by innovation, the role of regulators is no longer limited to oversight but has evolved to strike a balance between fostering innovation and ensuring that robust security measures are in place to protect every stakeholder, from consumers to enterprises.

[3] https://digipay.gov.in/dashboard/
[4] https://digipay.gov.in/dashboard/
[5] https://www.cnbctv18.com/business/finance/upi-fraud-cases-rise-85-pc-in-fy24-increase-parliament-reply-data-19514295.htm
[6] https://website.rbi.org.in/documents/87730/123044638/6OperationsandPerformanceofCommercialBanks.pdf
[7] https://www.npci.org.in/statistics/bd-td-and-uptime
[8] https://digipay.gov.in/dashboard/
[9] https://rbihub.in/mule-hunter-ai/

02

Payments security: Pioneering innovations, regulatory mandates, and global best practices in India

The payments ecosystem landscape today is akin to a mosaic of players that together drive innovation and financial inclusion. At the heart of this mosaic are fintechs, which are revolutionizing traditional models with innovative products and services where innovation meets heritage. From digitally issued cards to seamless cross-border payments and advanced KYC processes, they are redefining possibilities in financial services. Fintechs not only challenge established institutions but also serve as catalysts, enabling an ever-expanding array of digital products that cater to a diverse customer base.

A Mosaic of Players, A Maze of Security

While the number of innovations through new products and services are testament to progress, it is also observed that a distinct path has taken shape that is divided into multiple segments, each representing a distinct process or technology layer managed by different entities.

Let us consider the customer onboarding process. Prospective customers might first interact with the fintech company's intuitive application interface, then pass through a third-party digital identity verification service, and finally have their details processed by a bank. Each step involves different protocols, technologies, and security measures. In an ideal world, these disparate systems would ensure that the highest security standards are uniformly applied. In reality, however, gaps and inconsistencies often emerge. This scenario is even more untenable in an environment of evolving cyber threats. Flourishing innovation also brings with it an intricate maze of security challenges, which leads to 'security disparity.' Examples include:

- A mindset that leads to viewing security as a mere compliance exercise, a "tick-in-a-box" activity rather than a continuous, strategic investment
- Reliance on limited number of technology service providers leading to systemic vulnerabilities in the ecosystem
- Lean security teams and limited budgets, which hinder organizations' ability to implement and maintain comprehensive security strategies

'Security disparity' is most evident during transactions processing. As a customer initiates a payment, the transaction traverses several layers or 'hops' ranging from the merchant's gateway to various payment intermediaries to the acquiring bank and ultimately to the issuing bank. At each juncture, the integrity and robustness of security protocols can vary significantly. One system might employ state-of-the-art encryption and real-time fraud detection, while another might rely on older, less stringent measures. The result is a patchwork of security defenses that, while collectively robust, can individually leave room for vulnerabilities when not properly harmonized.

The key to overcoming this maze of security challenges lies in fostering greater collaboration among all stakeholders. Fintechs, traditional banks, payment intermediaries, technology providers, and regulators must work together to bridge the gaps in their respective systems. By establishing integrated security frameworks and interoperable standards, the industry can ensure that every hop in the customer journey upholds the same high level of protection. This holistic approach will not only mitigate risks but also enhance consumer trust and streamline the overall payment experience.

Securing payments systems by establishing baselines

Recognizing the potential of innovations, the RBI has recalibrated its policies to meet new challenges. Under its Payments Vision 2025, designed on the core theme of 4Es – E-Payments for Everyone, Everywhere, Everytime – is reinforcing India's position as the global leader in digital payments domain. The approach adopted by regulators is characterized by a collaborative spirit where dialogue between regulators and regulated entities is key. This ongoing engagement helps shape policies that are both practical and forward-looking by soliciting and incorporating industry feedback ensuring that regulations are reflecting the real-world challenges and threats.

Below are a few notable initiatives taken over the past few years:

1 Mandating EMV and Additional Factor Authentication (AFA)

By shifting from magnetic stripe cards, which were highly susceptible to cloning and skimming, to EMV-enabled cards, was a key step in combating skimming and card cloning fraud. Fraud rates have shown a significant decline in recent years. Introduction of additional factor authentication (AFA) for domestic card-not-present (CNP) and card-present (CP) transactions has provided an additional layer of defense, dynamically assessing risk. AFA measures such as device fingerprinting, geo-location tagging, behavioral pattern analysis , OTPs or biometric verification are also extended to digital payment channels to protect online and mobile based transactions. These initiatives have been instrumental in protecting consumers and financial institutions alike, and they remain a critical part of defense as digital transactions continue to expand.

2 Cross-border AFA: A novel move with global resonance

As per a recent survey by a social platform , over 47% users have faced financial fraud in the past three years and around 50% of users have reported unauthorized charges on their credit cards by both domestic and international merchants. Recognizing the complexities of international commerce, India has taken a bold step to extend its AFA mandate to cross-border CNP transactions. Regulatory frameworks in the EU – under PSD2 (Second Payment Services Directive) – and Saudi Arabia mirror this. Cross-border AFA hinges on global merchants being 3-D Secure (3DS) ready to meet stringent requirements. While this move may increase costs for merchants and impact transaction success rates initially due to additional authentication steps, the enhanced security benefits far outweigh these challenges. The increased friction can be considered by a necessary trade-off in a global landscape where payment security is paramount.

3 Increasing importance of integrated fraud intelligence

Regulators have now mandated non-bank payment system operators to put in place a real-time fraud monitoring solution to identify suspicious transactional behavior and generate alerts. While this regulation has boosted the card network initiatives in actively communicating transaction fraud alerts to issuers and acquirers, it has also forced other payment system operators to step up and communicate transaction fraud alerts to the ecosystem participants.

While many banks have existing fraud monitoring set-ups, the effectiveness of these systems remains inconsistent. The effectiveness of the alerts is largely dependent on the subsequent actions taken by these entities. There remains a gap between the transmission of fraud alerts and the prompt, effective remediation actions by issuers and acquirers. For instance, when a card network notifies a bank about a potential fraud, but the latter ignores it, the possibility of minimizing the impact gets minimized. If another bank promptly acts on the alert, the area of impact is reduced. The example underscores a critical gap between alert transmission and effective response. Bridging this gap is essential for maintaining trust and ensuring that fraud prevention measures are not only communicated but also fully executed.

4 Need of evolving security standards: Beyond PCI DSS

RBI's regulation on Digital Payment Security Controls in 2021 renewed the focus on Payment Card Industry (PCI) standards, including PCI Data Security Standards (PCI DSS), PCI PIN Transaction Security (PCI PTS), PIN management, point-to-point encryption (P2PE) and hardware security modules (HSM). The latest version of PCI DSS standard – version 4.0.1 – represents a significant update aimed at enhancing payment data security globally through risk-based approach. Organizations were provided the transition timeline from PCI DSS v3.2.1 to v4.0.1 to familiarize themselves with the updated standards and implement necessary changes till 31 March 2025. While the existing standard focuses on card payment security, there is a growing need for a security standard similar to PCI DSS specifically designed for protecting Virtual Payment Addresses (VPAs) and other unique digital payment credentials which have become central to digital transactions.

5 Tokenization across payment modes

The rapid adoption of card tokenization is transforming how transactions are secured by replacing the actual card numbers with tokens to minimize the risk of data breach. India is one of the early adopters of tokenization in card payments. With the widespread implementation of tokenization protocols, tokenized card transactions have surged. However, traditional guest checkout methods are still prevalent in certain pockets. The growth in card tokenization reflects the confidence that both consumers and merchants have in the security it provides.

The experience can be leveraged to adopt a similar tokenization methodology for other payment modes, specifically UPI and mobile wallets. Unifying tokenization security standards across cards, mobile wallets, and real-time payments will create a consistent and robust security framework for the entire payments ecosystem.

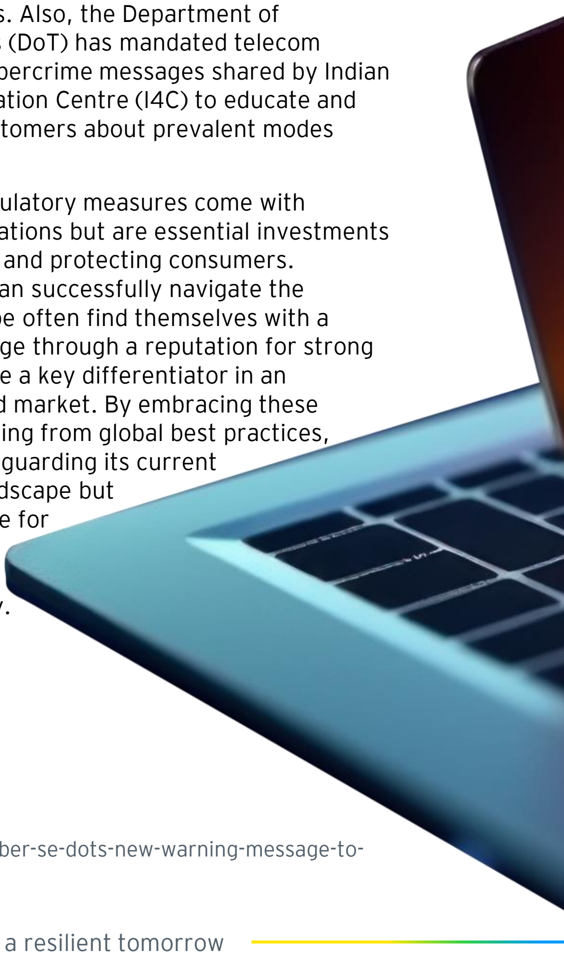
6 Regulatory interventions: Elevating fraud risk capabilities and broadening oversight

To fortify the digital payments ecosystem, RBI has introduced stringent requirements such as mandating the implementation of advanced fraud detection measures and the strengthening of KYC compliance across all transaction channels. Ecosystem participants are responding by integrating specialized tools to incorporate behavioral biometrics, geo-tagging, and AI-driven fraud risk scoring to proactively identify and mitigate fraudulent activities. Notably, RBI's Central Payment Fraud Information Register (CPFIR) initiative extends these enhanced regulatory standards to include payments ecosystem participants, thereby broadening the scope of oversight and fostering a more inclusive and resilient payments ecosystem.

7 Enhancing customer protection initiatives

Regulators have introduced accessible Dispute Resolution Systems which streamline the redressal process and ensure transparent handling of transaction disputes raised by customers. Complementing this, programs such as 'DigiSaathi' are empowering consumers by enhancing digital literacy and equipping them with best practices for performing secure transactions digitally. Additionally, the RBI's 'BE(A)WARE' campaign plays an important role in educating users about fraud risks and effective preventive measures. Also, the Department of Telecommunications (DoT) has mandated telecom operators to play cybercrime messages shared by Indian Cybercrime Coordination Centre (I4C) to educate and regularly remind customers about prevalent modes of frauds[10].

India's proactive regulatory measures come with potential cost implications but are essential investments in preventing frauds and protecting consumers. Organizations that can successfully navigate the compliance landscape often find themselves with a competitive advantage through a reputation for strong security which can be a key differentiator in an increasingly crowded market. By embracing these challenges and learning from global best practices, India is not only safeguarding its current digital payments landscape but also setting the stage for a more secure, innovative future in payments security.



[10] https://timesofindia.indiatimes.com/technology/tech-news/saavdhaan-agar-aapko-anjane-number-se-dots-new-warning-message-to-reliance-jio-airtel-and-vodafone-idea-subscribers/articleshow/116601020.cms

03

Securing the payments ecosystem: Addressing the commonalities and diversity of payments participants

As India's digital payments landscape continues its rapid evolution, ensuring robust security across both card transactions and emerging digital channels has become paramount. Over the last decade, the Indian payments environment has become much more dynamic, creating opportunities even for entities not associated with financial services to enter the ecosystem as payments service providers or payments service operators. The payments ecosystem is a unique composition of regulated entities and unregulated payments participants thereby increasing the complexity in establishing security baselines.

While the evolving regulatory landscape in India has been responsible in reshaping how each stakeholder in the payments ecosystem operates, the challenge has been in extending the ambit of the regulatory requirements to the non-regulated entities. While the onus of regulatory compliance remains with the regulated entities, the mandates on baseline security requirements has created somewhat of a shared responsibility model between the regulated and unregulated entities within the payments flow.

While security maturity varies across the ecosystem, the security risks impacting payments systems are similar. The attacker's focus is to siphon off funds and, typically, the weakest links are targeted. While targeting consumers through social engineering and Authorized Push Payment (APP) attacks has been a traditional favorite of attackers, the recent attacks have targeted payments intermediaries and supply chain vendors. There is usually a delay in detection of these types of attacks, which gives attackers more time to operate and also leads to larger financial losses for entities with the potential to impact multiple entities in the payments ecosystem.

While attackers use increasingly sophisticated techniques and the attack surface continues to grow with the expansion of the threat landscape and technology platforms used by the payments ecosystem, incident trends show that it is still the fundamental security controls and risks that are targeted by the attackers.

A recent trend in cyber-attacks is to attack an organization's service provider / vendor or less secure entities in the organization's supply chain. Such attacks, known as supply chain attacks, have targeted some of the big names in the security and technology space in the last one year. A few of these entities have also been service providers to multiple entities within the payments ecosystem in India. While there has been no report of a direct impact on digital payment transactions due to these incidents, it has raised concerns around the systemic risk associated with such vendors. That an attack on a single vendor or a fintech could impact multiple entities only aggravates the risks for payments entities that integrate with fintechs and other service providers, as is the norm. However, it is worthwhile to note that while supply chain risks are much discussed at present in terms of cyber security, they are not new for the payments ecosystem.

There have been incidents related to UPI and IMPS products where multiple banks were impacted since the product was provided by the same technology service provider. The recent ransomware attack on a fintech company in July 2024 not only impacted banks but also brought down connectivity between banks and NPCI[11].

In another recent case reported in India, an entity in the financial sector was defrauded amounting to losses in multiple crores in 15 days by miscreants who exploited a vulnerability in a payment gateway application provided by a fintech firm. The fraudsters, posing as customers, were able to edit the amount to be paid after the transaction was processed on the entity's application. While this incident was reported, the attackers could also have followed the same modus operandi at other financial institutions that were integrated with the same fintech payment gateway.

In a globally reported cyber incident, a payment gateway was hit by a cyber-attack that led to exposing credit card details of 1.7 million individuals[12]. The data breach included card numbers, card expiration dates, names, and addresses. If a similar incident were to happen in India today, the payment gateway would be liable to pay a hefty penalty as per the provisions of the DPDP Act 2023. An alert from I4C in October 2024 highlights the emergence of illegal payment gateways in the country created by organized transnational cyber criminals. Such a nexus where mule accounts are used and exploited to facilitate money laundering activities highlight the need to have an integrated approach towards security and fraud management.

Evolving fraud and cyber risk management in the digital payments ecosystem

Technology innovation and influx of new ecosystem participants have fundamentally transformed the digital payments landscape. With the surge in digital transactions, from UPI and mobile wallets to cross-border transfers, there has been an equally significant increase in the focus on fraud and risk management. Payment participants now employ specialized monitoring applications that dynamically assess transaction risks. Advanced measures such as step-up authentication and adaptive authentication have become essential tools ensuring that suspicious activities are intercepted before they result in significant losses. Additionally, card networks have geared up to provide a specialized services for fraudulent transactions monitoring. However, a lot remains to be done to safeguard customer interests as victims of these digital payment frauds.

Despite these robust measures, fraudulent activities continue to rise. For instance, according to the RBI's report "Operations and Performance of Commercial Banks" dated 26 December 2024, a staggering 85% of the cases identified in the first half of the current financial year were related to digital payments ecosystem while there was an increase of 130% on the number of frauds between 2022-23 and 2023-24[13]. This alarming statistic highlights the dynamic and evolving nature of fraud. Fraudsters are constantly refining their techniques and are leveraging sophisticated AI tools and exploiting system vulnerabilities resulting in a persistent escalation of fraud incidents.

[11] https://www.npci.org.in/what-we-do/upi/uptime-upi-month-wise
[12] https://www.paymentsjournal.com/payment-gateway-reveals-hack-affecting-1-7-million-cards/
[13] https://website.rbi.org.in/documents/87730/123044638/6OperationsandPerformanceofCommercialBanks.pdf

The key reasons for the emergence of the trend are constantly evolving tactics of fraudsters and, critically, the disjoint nature of cyber and fraud detection and response capabilities. Another key aspect related to payments fraud management is most of the fraud management solutions available today cater to card-based fraud use cases. There is a need to also build capabilities and solutions to address the requirements related to RTP fraud monitoring. While the regulatory body is facilitating initiatives around UPI fraud monitoring as well as setting transaction limits, introducing dynamic QR codes and friction in RTP products for high-value transactions, a lot more can be done at an ecosystem level to manage RTP related frauds.

In many organizations, even as advanced fraud prevention technologies are implemented, the systems often operate in silos. This lack of coordination means that while one part of the ecosystem might be successfully detecting fraudulent patterns, another is slow in responding or even unaware of the threat. For example, a transaction flagged by a bank's internal monitoring system might not trigger a timely response from an associated partner bank or fintech provider due to misaligned protocols or incompatible systems. Such fragmented approaches can delay intervention, allowing fraud to occur despite significant investments in security technology.

As the digital payments ecosystem is expanding, it is becoming increasingly evident that an integrated, holistic approach is needed which leverages the capabilities across the ecosystem. By harmonizing cybersecurity measures with real-time fraud detection and response systems, the industry can build a unified defense mechanism. Collaborative initiatives, such as industry-wide integration of data analytics across all channels, from the card networks to digital payment platforms, and threat and fraud intelligence sharing will ensure that every transaction is scrutinized under a consistent set of security standards, dramatically reducing the risk of fraud.

As digital payments continue to drive economic growth, the need for robust, coordinated fraud management systems becomes ever more critical. By embracing an integrated approach, financial institutions and technology providers can not only stem the tide of fraudulent transactions but also enhance consumer trust and ensure a secure, resilient payments ecosystem for the future.

While as a country we take great pride in other economies adopting the India payments stack, it is also important to note that it is also the same set of risks that are being exported to global payments products. Fintech firms, due to their in-depth knowledge of the India payments stack, would be service providers of choice for global entities as well. It is essential that such entities evaluate and assess the security risk posture and conduct a detailed due diligence prior to on-boarding fintechs for such requirements. This will help in limiting the cascading impact of known risks in the global ecosystem.

While the above instances demonstrate the risks associated with fintechs and technology service providers, innovation in the space of digital payments is largely driven by such entities. Hence, the issues related to lack of governance, inadequate security baselines, lean teams and security budgets, missing fundamental controls such as recon and monitoring in these entities need to be addressed on priority. While the regulated entities continue to own the responsibility of governance, it may be more efficient to govern this ecosystem through a Self-regulatory Organization (SRO). Establishing an SRO would not only support the creation of a strong security baseline as a mandate but could also provide a centralized avenue for security services that could be leveraged by the smaller entities.

Hence, while planning ahead, the cyber risks need to be addressed collectively by the ecosystem. While a one-size-fits-all approach will most certainly fail for such a dynamically changing payments ecosystem, the ability to establish strong security baselines, correlate risks, identify dependencies and vulnerabilities in the integrated technology platforms will enable a more secure digital payments flow.

04

Payments resiliency: Preparing for the next wave of digital payments adoption

As digital payments become increasingly central to economic activity, any disruption can have wide-ranging consequences for consumers, businesses, and financial institutions. Resiliency means ensuring that transaction systems remain operational, secure, and reliable no matter what challenges arise. Today, users prioritize robust system and availability as the key factor when choosing a service provider. Hence, the ability of payment systems to adapt, recover, and continue functioning seamlessly in the face of disruptions is crucial. Payments resiliency is not merely about preventing fraud or ensuring security, it is about creating an ecosystem that can withstand a multitude of challenges, from cyber-attacks and technical failures to market fluctuations and unforeseen crises.

The disruptions underscore the fragility of even widely adopted payment systems, serving as a wake-up call for the industry as every minute of disruption results in a missed opportunity of processing that transaction through that mode of payment. In addition, new users are entering the digital payments ecosystem and this influx amplifies the consequences of any system disruption, as even minor outages or delays can have far-reaching impact on transaction volumes and user trust. Due to the interconnectedness of the payments ecosystem, disruption at one player can quickly cascade, affecting downstream operations. The same was observed recently during a recent ransomware attack on a service provider multiple cooperative and regional rural banks in India affecting ATM withdrawals and UPI transactions.

Strategies for enhancing payments resiliency

Consequences of inadequate resiliency are far reaching both in terms of visible impacts such as delayed payments or use of alternate mode of payments for both merchants and customers, and invisible impacts where every minute of downtime translates into lost revenue and diminished customer confidence. Addressing these issues, therefore, requires an industry-wide commitment to rigorous resilience, stakeholders can adopt several strategic approaches:

Enhanced regulatory oversight

Regulatory measures such as RBI's Digital Payment Security Controls (DPSC) and Cyber Resiliency initiatives for non-bank Payment System Operators (PSOs) are essential to level the playing field and ensure a consistent standard of resilience across all regulated entities. Payments ecosystem participants who are currently unregulated should also be considered. These measures can be complemented by regular industry audits to assess and improve system robustness.

Sectoral resilience assessments

Comprehensive sectoral resiliency simulations are essential for ensuring the robustness of entire ecosystem. Joint resilience simulations and stress tests can be utilized to evaluate the performance of interconnected systems, for example, an entire lifecycle and involved participants in real-world transaction flows, ensuring that PIN validation, OTP generation, and other critical components are stress-tested in unison. Learnings from Bank of England's simulation of severe economic shocks and operational disruptions and Institute for Development & Research in Banking Technology's (IDRBT's) cyber drills that simulate coordinated cyber-attacks can be leveraged.

Unified Security and Resiliency Frameworks

Define and establish an industry-wide standard that mandates a minimum baseline requirement for emergency recovery protocols to help minimize the risk of fragmented systems.

Advanced technology investment

Leverage cutting edge technologies like AI, ML and blockchain for predictive analytics, real-time monitoring, and swift anomaly detection. Such technologies enable rapid responses to potential disruptions and help forecast emerging threats.

Towards a resilient future in digital payments

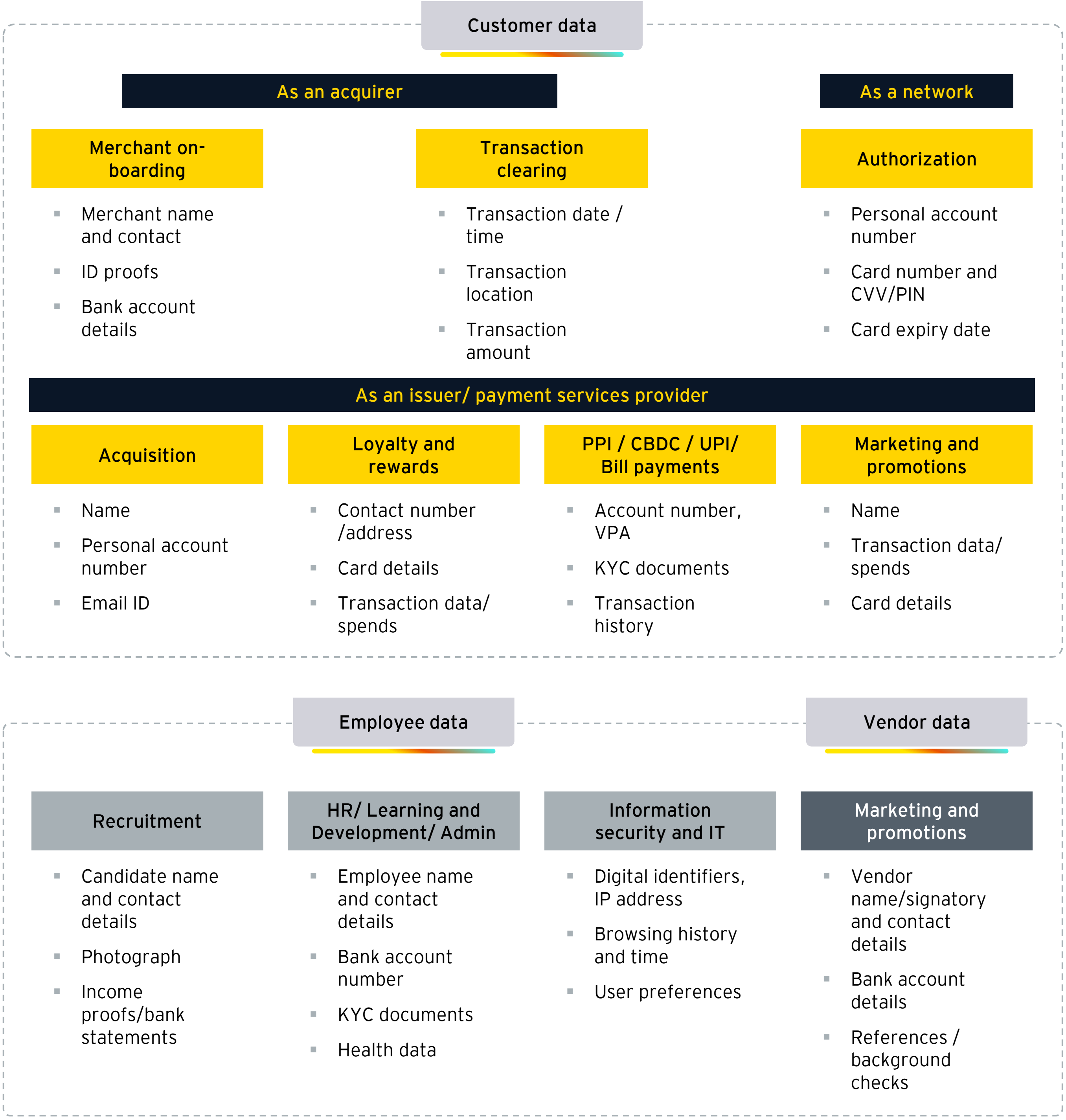
Payments resiliency is the cornerstone of a secure, efficient, and reliable digital payments ecosystem. The statistics on UPI and IMPS outages, the tangible impacts of bank-related security incidents, and the concentration risks from third-party dependencies highlight the urgent need for a unified approach. In embracing these strategies, India is not only addressing today's challenges but also laying the groundwork for a future where innovation and resiliency go hand in hand, ensuring a stable, inclusive, and thriving digital economy for years to come.

05

DPDP Act and Draft Rules: Impact on payments participants

As individuals increasingly adopt digital payments avenues, the data they generate create both an opportunity for payment companies to improve their customer engagement and a responsibility to keep customer personal data safe. The payments ecosystem in India today includes a diversity in scale and technology adoption as well as control maturity in terms of capabilities in safeguarding personal information. The DPDP Act, 2023 and the proposed DPDP Rules, 2025 will require payment companies to assess ways to maintain confidentiality and safeguard customer personal data. While planning compliance with this law, entities must consider this as an opportunity to revisit their data and security strategies and establish mechanisms that will boost customer trust, enhance brand value and build a competitive advantage in the ecosystem.

Payments industry personal data touchpoints



Customer data

As an acquirer

Merchant on-boarding
- Merchant name and contact
- ID proofs
- Bank account details

Transaction clearing
- Transaction date / time
- Transaction location
- Transaction amount

As a network

Authorization
- Personal account number
- Card number and CVV/PIN
- Card expiry date

As an issuer/ payment services provider

Acquisition
- Name
- Personal account number
- Email ID

Loyalty and rewards
- Contact number /address
- Card details
- Transaction data/ spends

PPI / CBDC / UPI/ Bill payments
- Account number, VPA
- KYC documents
- Transaction history

Marketing and promotions
- Name
- Transaction data/ spends
- Card details

Employee data

Recruitment
- Candidate name and contact details
- Photograph
- Income proofs/bank statements

HR/ Learning and Development/ Admin
- Employee name and contact details
- Bank account number
- KYC documents
- Health data

Information security and IT
- Digital identifiers, IP address
- Browsing history and time
- User preferences

Vendor data

Marketing and promotions
- Vendor name/signatory and contact details
- Bank account details
- References / background checks

Tracing DPDP Act and Draft Rules requirements across the payments chain

While the requirements of the Act and the draft Rules continue to be deliberated upon and debated across the country, the payments ecosystem is uniquely positioned when it comes to interpretation and implementation. While each payment participant will have a role to play in managing the privacy requirements of customers, it will also lead to development of a shared responsibility model between entities. While, typically, the data fiduciary and data processor roles are envisaged at an entity level, in the case of the payments ecosystem, use cases and scenarios will need to be analyzed and assessed to define these roles and the associated responsibilities.

Issuers and acquirers

These entities will take on many of the responsibilities by virtue of managing the customer relationship and contracts. They will have to manage and own the requirements related to notice, consent management, handling of the data principal rights, and breach notification to the customers. However, the success of their privacy program will also be dependent on their ability to govern the capabilities of the payments participants they integrate with. Assessing the dependencies and revisiting contractual requirements with their ecosystem partners will help set the tone of the shared responsibility model.

Card payment networks

While it is safe to consider that the role of these entities for the core payments processes will be that of data processors, further analysis is required for the add-on / value-added services being provided by the card networks. In use cases where networks might be involved in determining the means of collection and processing personal data, albeit through an Issuer, leads to a shared fiduciary role along with the Issuers. While most of these entities have established global privacy frameworks that have been adopted, extending the framework to meet the requirements of the DPDP Act and associated Rules will need to be planned.

Payments intermediaries

As the name suggests, these entities are typically placed in between customers and merchants during the process of fund collection / transfer. While most of these entities are not directly responsible for the collection of personal data or are pass through platforms in the payments flow, they are the custodians of large volumes of personal data as payments system operators. Ensuring adequate security safeguards to protect personal data will be a key obligation that fiduciaries will impose on these entities.

Fintechs

In operating models where fintechs provide platforms in a service model, shared responsibilities would arise. A service models where the traditional fiduciaries such as banks operate in an outsourced / SaaS model with fintech partners in a 'co-branded' manner, is a classic scenario where both could be perceived as fiduciaries while the bank continues to own the customer relationship. Another area of focus where responsibilities would be shared between the entities would be that of managing the Data Principal Right requests. While the rights of grievance redressal and nomination would typically be handled by the entity managing the customer relationship, fintechs will also need to address requests related to right to access, correction, and erasure.

It is vital for fintechs to agree upon obligations and liabilities in the context of personal data protection with the entities that own the customer relationship. Such agreed upon obligations and liabilities will also be applicable on the sub-contractors / vendors that fintechs on-board. Hence, adequate due diligence and contracting with them will also be essential. Another area of focus for fintechs will be balancing customer experience with the consent management requirements. While many customer facing applications developed by fintechs in recent times have been focused on enhancing customer experience by optimizing number of clicks, inputs, etc., the way they handle notice and consent requirements will need to be planned. A three-click onboarding USP for customers is getting a plus one or maybe two.   A well drafted notice by a techno-legal team will help in enhancing customer trust. As we await clarity on the mandate of integrating with external consent managers, the feasibility of integrating with multiple such entities would need to be evaluated and tested as well as agreed upon with their clients.

1 Merchants and acquirers

- Roles and responsibilities of Data Fiduciaries
- Notice and consent management
- Integration with consent managers
- Managing data subject right requests and grievance redressal
- Implementation of security safeguards
- Breach reporting to Data Principals and the Board
- Governance of data processors

2 Issuers

- Roles and responsibilities of Data Fiduciaries and plan for activities related to Significant Data Fiduciaries
- Notice and consent management
- Integration with consent managers
- Managing data subject right requests and grievance redressal
- Implementation of security safeguards
- Breach reporting to data principals, the Board and the regulator
- Governance of data processors

3 Card networks

- Adherence with data processor obligations
- Assess applicability of use cases for fiduciary role and realign contracts for shared responsibilities
- Implementation of security safeguards
- Managing compliance of vendors
- Support Data Fiduciaries in addressing data subject right requests
- Data breach reporting to Data Fiduciaries and the Board

4 Fintechs

- Adherence with data processor obligations
- Implementation of security safeguards
- Managing compliance of vendors / sub-contractors
- Support Data Fiduciaries in addressing data subject right requests through defined SLAs
- Data breach reporting to Data Fiduciaries and the Board

5 Payments intermediaries

- Adherence with data processor obligations
- Implementation of security safeguards
- Managing compliance of vendors / sub-contractors
- Support Data Fiduciaries in addressing data subject right requests
- Data breach reporting to Data Fiduciaries and the Board

In summary, while clarifications and amendments are expected based on the draft Rules, the payments ecosystem should initiate the activity of analyzing use cases and establishing the accountability model across entities. Building technology platforms that are centered around security and privacy by design will not only become an imperative but will also be a key business driver for the payments participants.

A privacy governance office is needed to drive and sustain privacy implementation. As awareness will continue to grow in the country, entities will need to scale up their capacity to manage and address data principal rights. For this, implementation of solutions for data discovery and traceability will be key. Based on their experience of implementing device and card-on-file tokenization, this ecosystem could also become trendsetters in implementation and adoption of personal data tokenization.

06

GenAI: New-age threats and the Art of Possible to secure digital payments

In the evolving world of digital payments, Generative AI (GenAI) is emerging as a game-changer and a formidable challenge. On one hand, it can streamline fraud detection, automate compliance, and enhance financial security through intelligent automation, while on the other, it equips fraudsters with sophisticated tools that enable them to craft hyper-personalized attacks at scale. Cybercriminals are no longer confined to basic phishing attempts. Instead, they use AI-powered tools that elevate the threat landscape. This evolving dynamic has sparked an AI arms race between financial security teams and cybercriminals where the cost of losing the advantage is measured in lakhs (if not crores) in fraud losses.

In this context, it is imperative for the industry to harness the benefits of GenAI while continuously innovating to outpace emerging threats, ensuring that the digital payments ecosystem remains resilient and secure.

How GenAI is supercharging payment fraud: The dark side of AI

01 Hyper-realistic impersonation: The new frontier of deception

Gone are the days where cybercriminals relied on poorly drafted emails. Today, GenAI-powered deepfake technology enables fraudsters to create ultra-realistic videos, images, and voice recordings that can fool even the most vigilant security teams. For instance, a finance professional at a multinational firm was deceived into transferring US$25 million after receiving a deepfake video call that perfectly mimicked the company's CFO[14]. The sophisticated impersonation bypassed internal controls, leading to significant financial loss before the breach was detected. In this evolving landscape, cybercriminals no longer need to infiltrate systems directly; convincing deepfakes can undermine security measures from within.

02 Synthetic identities and AI-generated data fabrication

GenAI is now used to create fake digital personas complete with dummy IDs, addresses, and transaction histories. These synthetic identities are then used to open fraudulent bank accounts, get illegitimate loans, or execute large-scale money laundering. Complex scams such as 'Pig butchering' scams, where criminals build trust over time before draining victims' funds, have become more automated, scalable, and harder to detect due to AI-generated fake profiles.

03 AI-enhanced phishing, vishing and email fraud

AI has elevated phishing techniques by enabling highly personalized scams. Fraudsters can now mine data from social media, company records, and leaked databases to generate accurate emails and voice calls that are convincing. AI-generated communications can mimic a CEO's writing style or replicate the voice of a trusted colleague, making it increasingly challenging for recipients to discern legitimate messages from fraudulent ones. This shift from generic spam to hyper-targeted, persuasive scams significantly increases the likelihood that victims will inadvertently authorize fraudulent transactions.

04 AI-Driven Cybercrime Tools and Polymorphic Malware:

The emergence of AI-powered malware has significantly increased the level of cyber threats. Polymorphic malware (like BlackMamba) can re-write its code in real-time, making it nearly impossible for traditional security tools to detect[15]. Specialized AI models such as FraudGPT and WormGPT now enable cybercriminals to easily generate undetectable hacking scripts, crack passwords, and automate large-scale fraud campaigns. This dynamic threat environment, where malicious code adapts in real time, presents a formidable challenge for conventional security systems tasked with protecting digital payments.

Fighting back: How the industry is using GenAI to combat fraud

Today, financial institutions, regulators, and fintechs are harnessing the power of GenAI to proactively counter increasingly sophisticated fraud schemes. By deploying advanced AI solutions, industry leaders are transforming GenAI into a critical tool for detecting and preventing fraudulent activities, usually before significant losses occur.

01 AI-driven fraud detection and prevention

Modern AI tools now analyze millions of transactions in real time, identifying subtle anomalies and suspicious patterns across various channels, including credit cards, UPI payments, and real-time transfers. For instance, if a customer who typically makes local purchases suddenly initiates a large international transfer at an unusual hour, the system can immediately flag the transaction for further verification. This predictive capability not only detects fraud as it happens but also anticipates potential threats before they escalate.

[14] https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

[15] https://www.hyas.com/blog/blackmamba-using-ai-to-generate-polymorphic-malware

02 AI-powered mule account detection

A significant challenge in the fight against fraud is the identification of mule accounts that are used for money laundering. Advanced AI models analyze transaction data, behavioral patterns, and account activities to detect indicators of money laundering, which exemplify this approach by pinpointing suspicious accounts linked to fraudulent networks, enabling timely intervention and disruption of illicit activities.

03 Advanced threat intelligence

Understanding the tactics of fraudsters is critical to devising effective countermeasures. Financial institutions are now deploying AI-powered threat intelligence platforms that continuously track and analyze fraud trends. They provide insights into emerging fraudulent techniques, thereby enabling organizations to adjust their security protocols dynamically and stay ahead. It is often said, "think how a fraudster thinks" to combat them.

By integrating advanced AI-driven strategies, the industry is not only enhancing its ability to detect and prevent fraud but also reinforcing the overall security and resilience of the digital payments ecosystem.

The "Art of Possible": Innovative ways GenAI can enhance payment security measures.

As GenAI continues to evolve, the Indian payments ecosystem should not only stay ahead of increasingly sophisticated cyber threats but also proactively transform the security landscape. Many entities are developing GenAI into a digital fortress that can be used to adapt, outsmarts and outplay cybercriminals. GenAI's integration with fraud prevention is embedding security intelligence during the transaction lifecycle.

01 AI-powered autonomous transaction firewalls

Imagine a next-gen firewall that analyzes real-time transactions, identifies anomalies, and dynamically thinks whether the transaction should be allowed or not, instead of directly blocking transactions. When an unusual activity is detected, additional authentication measures such as voice biometrics, contextual verification, or supplementary security prompts can be triggered, ensuring that any suspicious behavior is scrutinized before the transaction is allowed to be completed.

02 Invisible authentication with Risk-aware Digital ID

What if the user's behavior, such as style of typing, swiping, and interacting with payment apps, can be used to authenticate the user? AI can now track keystroke patterns, typing rhythm, swipe gestures, and even the way a person holds the phone to continuously authenticate in the background by creating a Risk-aware Digital ID that is ever evolving. This seamless, background authentication process means that even if a fraudster manages to intercept one-time passwords or other credentials, they still cannot replicate the nuanced behavior that uniquely identifies the user.

03 AI-powered fraud honey traps

From reactive actions to more proactive actions, AI-generated fake fraud victims can engage scammers in conversation, gathering intelligence on their tricks, current methods, and tactics-in-the-making to refine and update the security solutions in place. These AI systems can even convince fraudsters to reveal their bank details, QR codes, and payment networks, feeding this information directly into a centralized national anti-fraud blacklist.

As India's digital payments ecosystem grows, the battle between AI-driven fraudsters and AI-powered security systems is intensifying. The bottom line is that while fraudsters are getting increasingly sophisticated, organization's defenses are evolving in tandem. By leveraging AI-powered fraud detection, behavioral biometrics, dynamic security systems, and predictive threat intelligence, financial institutions are building the next generation of fraud defense. In this AI arms race, only the most adaptive, intelligent, and proactive systems will win.

07

Planning ahead: The next in payments security and resilience

As the payments ecosystem plans ahead and prepares for the next wave of digital payments adoption, this is an opportunity to innovate, collaborate, and manage risks in a more effective way. As attackers continue to use modern technology platforms and tools as enablers, the ecosystem will need to become more proactive in preparing for the new-age risks anticipated.

State-sponsored attacks on payments channels:

While state-sponsored cyber-attacks have been observed in the past, such an attack on a digital payment channel could have a crippling effect on the economy. Predictive monitoring and security analytics, a collaborative approach to correlating threat intelligence and improved visibility on threats and risks across the payments flow will become critical to manage and minimize the damage caused by such attacks.

AI-based attacks:

The impact of AI-based attacks has already been seen in the payments ecosystem. However, these are expected to continue to increase in severity of impact and complexity in detection and response. Strengthening of continual monitoring, stronger process and governance controls, and use of effective AI-based security solutions will help in building a more resilient payments product.

Blockchain:

Blockchain holds significant potential in shaping the future of payments, both in terms of security and speed. The benefits of the technology can be leveraged to increased transparency, faster settlement times, and reduced reliance on intermediaries, especially in cross-border payments and peer-to-peer scenarios. While payments players have started developing use cases such as digital identity verification, stablecoins and digital currencies, and tokenization of sensitive payment data and assets, further impetus to drive adoption will be required in the ecosystem. Immutable ledgers, smart contracts and increase in auditability will drive accountability across entities. Cross-border payments and settlements could see a significant increase in speed and also become near real-time, thereby enhancing business efficiency as well.

Friction in payments products:

While the initial view has been to make payments frictionless from a customer experience perspective to enhance adoption, product teams are also pivoting to strategies to include friction during the customer journey to enable fraud and risk monitoring controls. It is essential to manage the introduction of such features in the payments products in a way that keep customers engaged while providing the entities to manage and reduce fraud risks in real-time payments products.

Stronger risk analytics:

Predictive risk analytics will be instrumental in managing payments frauds. Enhancing capabilities on behavioral pattern analysis, spend analytics, correlating between business patterns, technical events and fraud patterns can help in managing payment frauds more effectively. Device-based risk identification is a new area that can be explored in terms of its potential in combatting payments fraud. However, balancing these activities with the privacy rights of consumers will be essential as well.

Collaboration across entities:

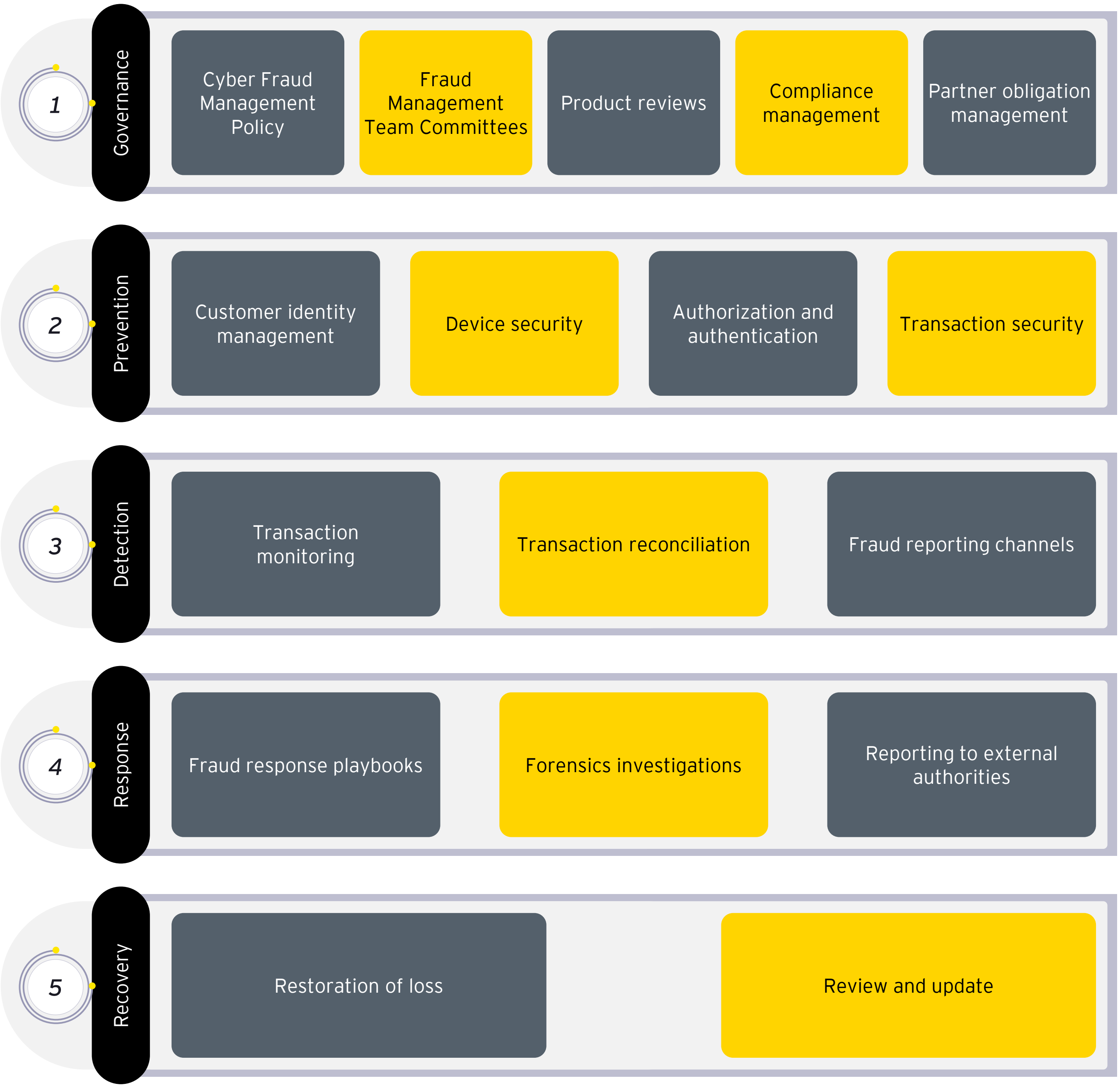
While individual entities continue to strengthen their security and resilience capabilities, it is also essential to address risks at the ecosystem level to build a resilient payment flow. Identifying interdependencies, security risks at a payment flow level and collaborating while planning security controls, solutions and frameworks will strengthen the security of the payments flow. A collaborative approach in solving the card and device tokenization has worked well for the ecosystem and can be used as a model reference for an ecosystem level risk management framework as well. Centralized implementation of new-age security solutions and a combined audit framework by the established payments entities could help entities such as smaller merchants, payment aggregators, and fintech companies enhance security and drive operational efficiencies.

Industry-wide collaboration on fraud intelligence:

Globally, the advantages of a collaborative approach to fraud prevention among financial institutions, regulatory bodies, and private sector ecosystem participants is widely recognized. One notable example is the Financial Services Information Sharing and Analysis Center (FS-ISAC), which unites banks, payment processors, and other financial entities to share real-time threat intelligence, ensuring a coordinated response to emerging cyber threats. Another example is related to SWIFT's Payment Control Services, which enable financial institutions to flag or block anomalous payments before they are made. In 2024, a pilot program was initiated to test a new approach that uses AI-based algorithms for detection of fraud in transactions based on historical data analysis. Such collaborative initiatives are key to transforming isolated alerts into actionable intelligence to ensure that the global payments ecosystem remains robust and secure.

Integrated cyber and fraud risk management:

While most payments entities have cyber security and fraud management capabilities, often, these functions operate in silos. To address new-age payments frauds, it is imperative to have an integrated capability for cyber and fraud risk management and response. The framework below is an indicative reference for adoption and can be leveraged by entities to enhance their cyber fraud management capabilities.



1 Governance
Cyber Fraud Management Policy
Fraud Management Team Committees
Product reviews
Compliance management
Partner obligation management

2 Prevention
Customer identity management
Device security
Authorization and authentication
Transaction security

3 Detection
Transaction monitoring
Transaction reconciliation
Fraud reporting channels

4 Response
Fraud response playbooks
Forensics investigations
Reporting to external authorities

5 Recovery
Restoration of loss
Review and update

Security, privacy and compliance by design:

Building payments products that are secure, compliant and safeguard personal data by design will not only help in driving operational efficiencies in the ecosystem but will be a key differentiator for fintechs and payments product providers to drive customer trust hence acting as a business enabler. A well-defined payments product security framework will enable technology and product teams to understand the requirements right from the ideation phase and will enable creation of requirements during their agile development cycles. Such a framework will also help them demonstrate their product features and capabilities to customers more effectively. The framework below is indicative and can be considered as a reference for further customization depending on the requirements of the payment product being built.

- Embed security into product development lifecycle
- Build multi-level fraud detection capabilities
- Plan for compliance by design
- Incident response and resilience
- Support merchant security
- Plan for grievance redressal and dispute resolution
- Govern security of fintechs and vendors
- AI Observability
- Safeguard customer PII and transaction data
- Drive customer awareness
- Design risk-based authentication mechanisms
- Supply Chain Risk Management

Contacts

For further details and information, our key contacts on these topics

Murali Rao
Partner and Cyber Security Leader, EY India

Email murali.rao@in.ey.com

Phone +91 8067270086

Kartik Shinde
Partner, Cybersecurity Consulting, EY India

Email kartik.shinde@in.ey.com

Phone +91 9867163368

Aniket Bhosle
Partner, Technology Consulting, EY India

Email aniket.bhosle@in.ey.com

Phone +91 9730081812

Manasi N J
Director, Technology Consulting, EY India

Email manasi.nj@in.ey.com

Phone +91 9892348249

Author

Parag Sanghvi
Manager, Technology Consulting, EY India

Girish Purswani
Director, Technology Consulting, EY India

Manasi N J
Director, Technology Consulting, EY India

Aniket Bhosle
Partner, Technology Consulting, EY India

Kartik Shinde
Partner, Cybersecurity Consulting, EY India

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

8th Floor, Building No. 14A
Block 14, Zone 1
Brigade International Financial Centre
GIFT City SEZ
Gandhinagar - 382 355, Gujarat
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 & 1st Floor
# 11, 'A' wing
Divyasree Chambers
Langford Town
Bengaluru - 560 025
Tel: + 91 80 6727 5000

3rd & 4th Floor
MARKSQUARE
#61, St. Mark's Road
Shantala Nagar
Bengaluru - 560 001
Tel: + 91 80 6727 5000

1st & 8th Floor, Tower A
Prestige Shantiniketan
Mahadevapura Post
Whitefield, Bengaluru - 560 048
Tel: + 91 80 6727 5000

Bhubaneswar
8th Floor, O-Hub, Tower A
Chandaka SEZ, Bhubaneswar
Odisha - 751024
Tel: + 91 674 274 4490

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

Delhi NCR
Aikyam
Ground Floor
67, Institutional Area
Sector 44, Gurugram - 122 003
Haryana
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

Jaipur
9th floor, Jewel of India
Horizon Tower, JLN Marg
Opp Jaipur Stock Exchange
Jaipur, Rajasthan - 302018

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

6th floor, Sector V,
Building Omega, Bengal Intelligent Park,
Salt Lake Electronics Complex, Bidhan
Nagar
Kolkata - 700 091
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

3rd Floor, Unit No.301
Building No.1, Mindspace-Gigaplex
IT Park, MIDC, Plot No. IT-5
Airoli Knowledge Park
Airoli West, Navi Mumbai - 400 708
Tel: + 91 22 6192 0003

18th Floor, Altimus
Pandurang Budhkar Marg, Worli
Mumbai - 400 018
Tel: + 91 22 6192 0503

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

10th Floor, Smartworks
M-Agile, Pan Card Club Road
Baner, Pune - 411 045
Tel: + 91 20 4912 6800

Ernst & Young LLP

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at Ground Floor, Plot No. 67, Institutional Area, Sector - 44, Gurugram - 122 003, Haryana, India.

EYIN2503-002
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

RG

ey.com/en_in

X @EY_India   in EY   YouTube EY India   f EY Careers India   @ey_indiacareers