

# MPAI

MERCHANTS' DAY CONFERENCE 2026

# BUILDING TRUST IN AGENTIC COMMERCE

ENABLED BY



24TH MARCH 2026

JIO CONVENTION CENTRE, MUMBAI

MPAI SECRETARIAT MANAGED BY KOAN ADVISORY GROUP

Merchants' Day, our flagship event, now in its fifth edition, was attended by participants and experts across organisations representing digital merchants, payment processors, card networks, regulators, technology, legal, and academia. The event looked at the opportunities and upcoming governance issues as AI agents start shaping the future of commerce.

Agentic AI systems that can discover, negotiate, and pay on behalf of consumers are no longer theoretical, they are being piloted and deployed. **The event was forward looking and examined current frameworks across payments infrastructure, legal and consumer protections that are needed to underpin these systems.**

Organised by	<b>MPAI</b>
Theme	<b>Building Trust in Agentic Commerce</b>
Date	<b>March 24, 2026   IST 9:30 AM - 4:30 PM</b>
Venue	<b>Jio World Convention Centre, Mumbai</b>
Powered by	

## Inaugural Session

### | MPAI Vision 2026

The event began with the MPAI Chair setting out priorities for the year, centred on ensuring that digital merchants are active participants in shaping and not merely spectators to the evolution of the digital payments ecosystem. Two major themes dominated the day's agenda: Agentic Commerce and payment interoperability.

### | Opening Address

**Sanjay Shripatrao Katkar (IAS)** - Managing Director, MahaIT

The Opening Address reaffirmed the depth and durability of India's digital public infrastructure and the government's commitment to further extending its benefits across the following areas.

- A clear arc was traced from Aadhaar's near-universal coverage (reaching virtually all 140 crore Indians) to the successive phases of BharatNet expanding fiber connectivity to the country's most remote corners. These are not abstract statistics, they are the foundation on which scalable, trusted digital systems, including agentic AI, can rely upon.
- Maharashtra's role as a commercial hub and a driver of digital infrastructure was highlighted, with MahaIT positioned as a 24x7 institution serving citizens at scale. Whilst IT infrastructure is largely in place, what is required is governance around identity, consent, accountability, and trust to ensure that the next wave of innovation, from autonomous payments to AI-driven commerce, extends benefits inclusively and securely.
- The importance of collaboration among technology platforms, infrastructure providers, governance bodies, and regulators was also stated in the address. When they align around shared goals, stronger trust, deeper adoption, and measurable contribution to GDP are seen to follow.





## | Merchants' Day Lecture

P Vasudevan  
Executive Director, RBI

## Segment 1: Agentic Commerce & Autonomous Payments



### | Case Study 1: Deploying Autonomous Payments for Smart Retail in India

#### Ishan Sharma

Head of Sales, JUSPAY

This case study mapped the shift from the familiar browse-cart-pay model towards intent-based, agent-to-agent commerce, where a consumer's buyer agent interacts autonomously with seller agents to research, negotiate, and complete transactions. While the technology is evolving rapidly, India's payments stack and regulatory frameworks need to catch up before they are fully able to support autonomous flows. The speaker suggested a hybrid, human-in-the-loop model as the realistic near-term path towards fully autonomous payments.

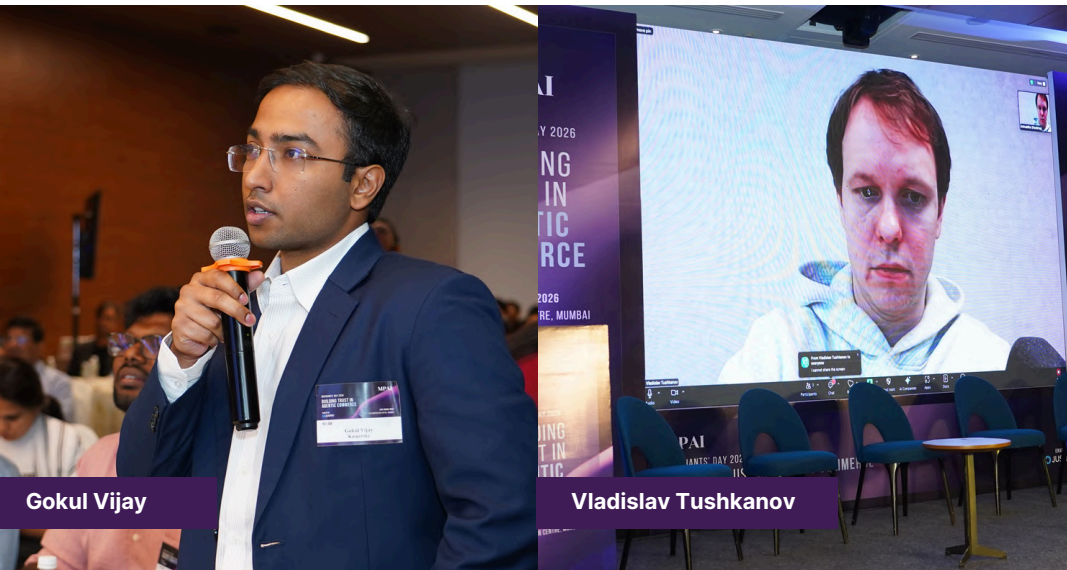
#### Insights:

- Commerce is moving from 'browse → cart → pay' toward intent-based flows where AI agents complete the entire purchase journey.
- LLMs (ChatGPT, Gemini, Claude) could become new marketplace aggregators, competing with merchant-specific and platform agents for customer ownership.
- Small sellers and direct-to-consumer (D2C) brands may find the costs associated with agent-based discovery lower when compared to building e-commerce storefronts and democratising access to customers.
- The current payments stack, built on fixed rules and limited context, is not fully equipped to handle dispute resolution or intent verification in agentic flows. Significant infrastructure upgrades are needed.

#### Existing challenges:

- Integration of modern authentication systems within the ambit of agent-initiated transactions, defining consent for autonomous spending, building auditability to reconstruct intent and resolve disputes.
- Emerging security risks such as prompt injection, rogue agents, and cartel behaviour among seller agents.
- Currently, agents assist with discovery and checkouts, humans remain in the loop for authentication and key confirmations. Full autonomy is still a few years away.
- Closed-loop wallets may find more use cases for agentic purchases than open-loop multi-party rails.

## Segment 1: Agentic Commerce & Autonomous Payments



### | Case Study 2: Making Agentic Commerce Secure

#### **Gokul Vijay**

Senior Government Affairs and  
Public Policy Manager, Kaspersky

#### **Vladislav Tushkanov**

Group Manager, AI Tech  
Research Center, Kaspersky

In their case study presentation, the team from Kaspersky showcased how security threats to Agentic Commerce are already active. The speakers presented documented examples of prompt injection on live marketplaces and silent memory manipulation via invisible web content. With legal precedents establishing merchant liability for chatbot behaviour, the session made a case for prioritising cybersecurity from the very onset.

### Insights:

- Product listings and vendor sites are already being optimised with hidden instructions that cater to AI agents, often overriding the actual intent of human users. This makes prompt injection a real issue that's affecting how we interact with these platforms.
- Agent memory is another active attack surface - invisible text in web content can silently poison an agent's stored context to serve advertising or brand objectives without user awareness.
- Legal precedents, such as the Air Canada chatbot case, establish that in the end it is the companies that are liable for agent-driven errors or fraudulent outcomes.
- Agent capabilities such as browsing, buying, and remembering are outpacing security and alignment. This is a dangerous developmental gap.
- When designing AI systems, it's better to use narrow, task-focused agents with limited permissions rather than powerful general-purpose agents. This approach reduces vulnerabilities and makes it easier to track and audit their behaviour.
- It is advisable to apply structured peer-reviewed frameworks, such as OWASP Top 10 for LLMs and agentic applications, to enumerate and mitigate common failure modes from the outset.



## Panel Discussion: Building Trust, Safety, and Scale for Agentic Commerce in India

Ishan Sharma - JUSPAY | Anand Panda - BillDesk | Rohan Bagai - AZB & Partners | Gokul Vijay - Kaspersky | Shantanu Shirke - Mastercard | Salil Mody - Meta (Moderator)

The panel examined the systemic conditions needed to make Agentic Commerce trustworthy at scale. Discussion spanned UX design, legal frameworks, payment network infrastructure, and industry governance. The conversation moved between the immediate (how does passkey authentication work in an agent-initiated flow?) and the structural (who is accountable when an agent acts wrongly?), converging on a shared view that the industry needs to move ahead of regulation while ensuring that governance, and not just technology, shapes the intended outcome.

### Insights:

- Designing interfaces that work for AI agents is a new challenge. Since traditional payment interfaces are built for humans, they often don't work well with agents. Merchants need to optimise their systems for both human and agent interactions to ensure a smooth user experience.
- Mastercard, for instance, is building a verifiable intent framework. A cryptographic signature that encodes who authorised what, for which merchant, at what value, offers a concrete mechanism for accountability in autonomous transactions through existing card rails.
- The shift from OTP to passkeys/biometrics is imminent. Agentic Commerce is accelerating this transition for the broader ecosystem.
- India's Digital Personal Data Protection Act, 2023 (DPDPA) was drafted for human data principals, not autonomous agents. There is no specific legal regime for automated micro-decisions in a commerce journey. Accountability between agent<>developer<>deployer remains ambiguous.
- Know Your Agent (KYA) will be a natural parallel to Know Your Customer (KYC). Agents will need verifiable, persistent identities with defined permission scopes, especially where sub-agents or multi-user configurations are involved.
- Payment agents should be treated as tightly permissioned workers, specific to merchant categories, capped transaction values, and explicit use cases, not all-access participants.
- Industry bodies like MPAI have a role in setting common guardrails, aligning narratives, and advocating for parameters-based frameworks over prescriptive rules.

## Panel Discussion: Building Trust, Safety, and Scale for Agentic Commerce in India

### Risk-based governance:

- Security controls should scale with reversibility, autonomy, and exposure of the agent action. Human-in-the-loop checkpoints must be meaningful, not performative.
- Cross-border complexity is a challenge, with Indian users, foreign LLMs, and merchants operating across different jurisdictions. Given India's growing digital presence, it has a unique opportunity to contribute to shaping global standards and norms in this space.

### Key barriers to mainstream Agentic Commerce:

- The main hurdles for Agentic Commerce to go mainstream are adoption, keeping regulations up to speed, building user trust, addressing accountability gaps, and dealing with varying industry standards.



## Segment 2: Payment Authentication and Tokenisation



### | Case Study 1: Interoperability and Tokenisation in the Case of Credit Cards

#### P Rajagopal

Head - Digital Payment Solutions and Agentic AI Payments, Visa

Visa looked at India's card payment system, which uses tokens for security but which is fragmented. It explored ways to bring the convenience of saved-card payments to smaller merchants. With 100 percent of Indian e-commerce card transactions tokenised but card-on-file (CoF) tokens locked to individual merchants. Device tokenisation and passkeys appear to be the near-term fix for a broader Intelligent Commerce framework that addresses the agentic future.

#### Insights:

- India leads globally on e-commerce tokenisation (63-65 percent of network-level transactions are CoF), but these tokens are merchant-specific, that is, they don't follow the consumer across sites.
- Device tokenisation - saving a card on a trusted payment service provider (PSPs) (such as PhonePe, Google Pay, or Cred) enables a saved-card user experience across thousands of small merchants without requiring CoF integration at each merchant.
- Approximately one in three card transactions are still guest checkouts. This takes about 2 minutes for manual entry and lowers the success rates. Passkeys (FIDO-based) cut checkout to 15-20 seconds with about 10 percent improvement in payment success rates.
- Passkeys abide by the RBI's Alternate Factor Authentication Directions, 2025 and act as an alternative to OTPs.
- For Agentic Commerce, Visa's Intelligent Commerce framework introduces agent tokens (agent-bound, non-portable if stolen), payment instructions (codified user intent, confirmed biometrically, usable in disputes), and a trusted agent signal at the network edge.
- Merchants must consider whether AI agents help or hinder business. If they're trustworthy and have a good track record with users, they might become a key way for businesses to connect with customers.

## Segment 2: Payment Authentication and Tokenisation



### | Case Study 2: Interoperability Across UPI Autopay

#### Kanishk Mehta

Senior Director, Razorpay

Using the history of railway gauge standardisation as its foundation, this case study explained that payments interoperability is inevitable. India is at an inflection point across three dimensions: interface (who initiates the payment), asset (which instrument is used), and user (who or what executes the transaction). The session was particularly focused on the near-term milestone of UPI autopay mandate portability, and on the longer-horizon vision of embedded finance and anticipatory, Agentic Commerce.

#### Insights:

- Every industry converges toward interoperability over time, as seen in railways, shipping containers, and the internet. Payments will follow a similar trajectory.
- There are three levels where payment systems are becoming more compatible:
  - **Interface:** Payments can be made from any app, on any platform.
  - **Asset:** Different payment methods like cards, UPI, and credit lines can be used together seamlessly.
  - **User:** AI agents or intermediaries can make transactions for users.
- UPI autopay mandate interoperability is expected to go live soon, enabling merchants to benefit from higher success rates, better uptime, and reduced dependency on specific PSPs.
- For consumers, mandate portability means faster, more reliable recurring payments and for PSPs, a shift from incentives to better user experience.
- The 'minus-one interaction' vision: payments that anticipate consumer's need before the consumer articulates it – is technically feasible. The bottleneck is user readiness, operational processes, and regulatory frameworks.
- The short-term impact of these shifts is often overestimated, but in ten years, the impact will be huge.



## Panel Discussion: The Future of Payments - Interoperability, Identity, and Zero-Friction User Journeys

**Kriti Trehan** - Data & Co - Law & Policy Advisors | **Kanishk Mehta** - Razorpay | **Ravi Rajagopal** - Adyen | **Rajagopal P** - Visa | **Mayur Wadpalliwar** - PhonePe | **Aniruddha Shanbhag** - MPAI (Moderator)

The last panel of the day covered the threads across the second segment, examining the practical roadmap for authentication and tokenisation over the next 12 to 18 months. The panel discussed the fundamental gaps between zero friction and meaningful user consent. The conversation oscillated between the immediate merchants deployments and user control when payments become invisible.

### Insights:

- Device tokenisation and passkeys can lift authentication success from about 86 percent toward 100 percent, and overall payment success rates from about 80 percent to 92 percent. The business case for immediate adoption is strong.
- Immediate action points for merchants:
  - Integrate with major device token requesters (PhonePe, Google, Cred)
  - Adopt passkeys/biometric authorisation
- Device tokenisation mirrors the UPI success model of one trusted app, one flow, user in control when applied to credit cards.
- 2026-27 is expected to be the anchor period for mobile Near Field Communication (NFC) in India, driven by affordable NFC-capable devices, mature bank risk systems, and improved consumer comfort. Historically, markets comparable to India saw around 2x improvement in the adoption of contactless payments following large-scale NFC deployments.
- Global authentication best practices relevant for India:
  - trusted device designation
  - network tokenisation
  - unified card view across online and offline for richer risk signals.



### Insights (Contd):

- Under DPDPA, consent must be free, specific, informed, unconditional and unambiguous. Zero friction and meaningful consent can be aligned if consent is treated as architecture instead of a compliance checkbox.
- To move from a decade of OTP conditioning to frictionless authentication requires clear communication, demonstrable limits, and accessible recourse.
- Design principle to follow:
  - Secure front-load consent at onboarding
  - Provide contextual nudges and transaction logs
  - Build revocability and dashboards into the product from day one.
- Tokenisation is evolving into an identity passport - it can carry context about the device, merchant relationship, and behavioural history. In Agentic Commerce, agent tokens will carry equivalent signals for agent identity and authorisation scope.
- Zero friction must not mean zero accountability. Every automated payment must be backed by explicit user intent, robust governance, and clear recourse mechanisms.

## Key Themes from Merchants' Day 2026

Across both segments, a set of consistent themes emerged that will shape the agenda for India's digital payments ecosystem in the near future.

**Governance must lead technology:** A recurring observation across sessions advocated that technical capability in agentic systems, tokenisation, and biometric authentication has leapfrogged the governance and legal frameworks that are necessary to inspire user trust and ensure accountability across the ecosystem. The open questions of identity, consent, accountability, and liability need to be answered through robust principle-based regulations.

**Interoperability is a structural challenge:** Whether in the instance of UPI autopay mandates, card tokenisation across merchants, authentication credentials across channels, or agent identities across payment networks, the demand for interoperability remains consistent. Fragmentation imposes costs that lead to friction, drops in adoption, and issues with dispute redressal, factors that ultimately impact merchants and consumers.

**Trust is built through control, transparency, and recourse:** Zero friction is a design goal, not an end in itself. The sessions consistently circled back to the insight that consumers will extend trust to automated and agentic payment systems only if they can understand what those systems are doing, set meaningful limits, and exercise genuine recourse when something goes wrong. Designing for trust is different from, and more demanding than, designing for user adoption.

**India is well-positioned to shape global standards:** India's combination of scale, fintech maturity, and regulatory sophistication gives it a meaningful seat at the table where global norms for agentic payments, agent identity, and cross-border accountability are being established. Several sessions noted that no single jurisdiction can govern this space alone, and that India's early leadership in areas such as tokenisation and UPI positions it well to contribute to the frameworks that will matter most.

**The near term belongs to human-in-the-loop:** Full agent autonomy in commerce and payments is a few years away. The practical opportunity in the next 18 months lies in deploying device tokens, passkeys, and biometric authentication, and enabling UPI autopay mandate portability. The Agentic Commerce infrastructure rails will also be built – agent vetting, verifiable intent, audit trails – that will allow autonomous flows to be introduced safely and incrementally as regulatory and consumer trust is established.



**Priyanka Maggu Chopra**  
Chair, MPAI



**Sumati Sapru**  
Co-Chair, MPAI



**Aniruddha Shanbhag**  
MPAI

# MPAI

The Merchant Payments Alliance of India (MPAI) a group of like-minded merchants accepting digital payments in an ever-growing digital market.

We serve as a platform for merchants to share information and expertise in a useful and efficient manner. For membership related queries please write to us at [aniruddha@merchantpaymentsalliance.in](mailto:aniruddha@merchantpaymentsalliance.in)

[WWW.MERCHANTPAYMENTSALLIANCE.IN](http://WWW.MERCHANTPAYMENTSALLIANCE.IN)

Secretariat managed by Koan Advisory Group

