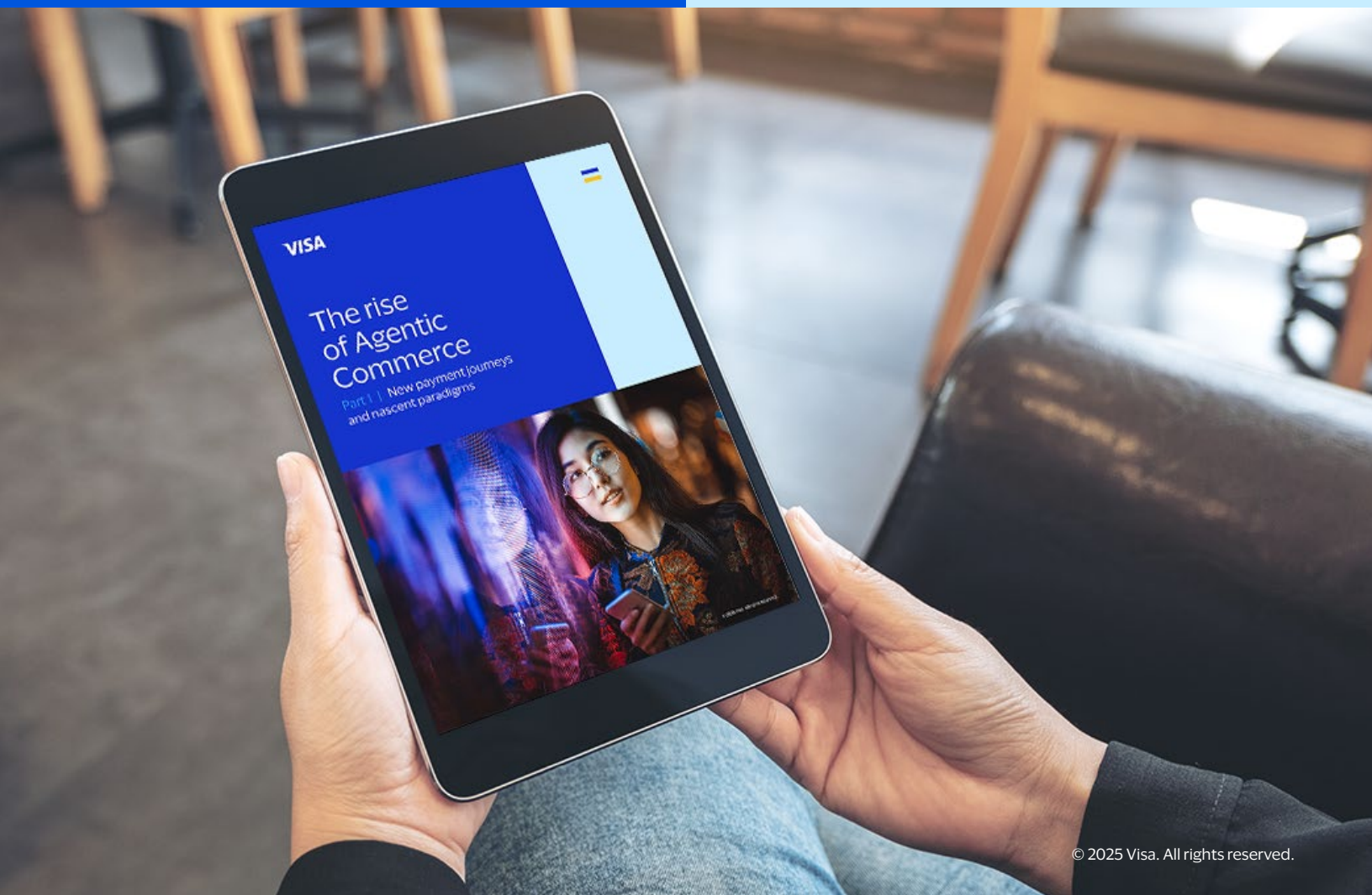
The rise of Agentic Commerce

Part 1 | New payment journeys and nascent paradigms

What's Inside



Introduction

Early AI models like OpenAI's GPT-2 (2019) and GPT-3 (2020) attracted widespread interest from the tech community. But it was the launch of ChatGPT in 2022 that marked a cultural turning point. The general public witnessed the power of generative AI to engage in human-like dialogue and help in real tasks.

Since then, AI development has accelerated at a dizzying pace. Model capabilities have grown exponentially, investment in AI infrastructure has surged and a wave of AI-powered software – from broad-purpose platforms to highly specialised tools – has captured the attention of consumers and businesses alike.

Amid the growing discourse on generative AI's impact, much attention has been paid to how it will transform productivity, its economic implications and the disruption of workforce dynamics – particularly within banking and financial servi es. But while we often explore how AI will reshape payments, far less has been said about the reverse: how payments themselves will shape the evolution of AI. This raises a fundamental question: How will we pay (and be paid) through AI apps and agent workfl ws?

As more powerful models, applications and agents arise, we expect payments to be an increasingly relevant gateway for purchases and transactions, paving the way for the era of 'Agentic Commerce'.

This paper is the first in a th ee-part series exploring that evolution

While this space is evolving rapidly – and some predictions may need recalibration – we believe that it's crucial to understand how payments could work seamlessly and securely in an AI-powered world.

Our objective with this paper is to stir thinking, provoke discussion and spark ideas that help the payment industry prepare for the next generation of eCommerce fl ws.

AI-powered commerce

The generative AI revolution can be traced back to a pivotal 2017 research paper by Google, which introduced transformer architecture and laid the groundwork for today's generative models. The public launch of ChatGPT in 2022 rapidly propelled these advancements into day-to-day use, attracting unparalleled levels of adoption, tech talent and investment.

Modern generative AI now supports multimodal inputs, exhibits increasing reasoning capabilities and integrates with other applications. General-purpose tools like ChatGPT, Claude, Gemini or Midjourney are complemented by specialised, vertical AI-first solutions – e.g. Cursor for coding, Sierra for customer support or Figma AI for design.

Next on the AI journey, autonomous agents begin to display the ability to perform tasks and make decisions with minimal human input.

At Visa, we believe that AI has the potential to reshape the future of e-commerce. From purchases initiated through an AI chat interface to agents transacting on our behalf, the possibilities are expanding.

To support this evolution, current payment infrastructure – designed around human interaction – will need to adapt. UI design, fraud controls, payment fl ws and compliance frameworks will require rethinking for agent-first inte actions.

This three-part report invites industry players to consider what's required to create frameworks, tools and rules for secure and scalable payment experiences, native to emerging AI workfl ws.

> "Soon people will have AI agents browse, select, purchase and manage on their behalf. These agents will need to be trusted with payments, not only by users, but by banks and sellers as well."
>
> **Jack Forestell**
> Chief Product and Strategy Officer, Visa[1]

How do we see AI-initiated payments evolving?

We see the evolution of agentic payments potentially unfolding through four stages. Each step builds on prior capabilities, leading from early-stage guidance to the possibility of autonomous transactions and orchestration.

AI Recommends → AI Initiates → AI Transacts → AI Orchestrates

Most of today's AI interactions sit in the first stage, AI Recommends, where AI functions as a smart advisor. Users query large language models (LLMs) for purchase suggestions, and in return, receive tailored recommendations based on prompts, preferences and prior interactions.

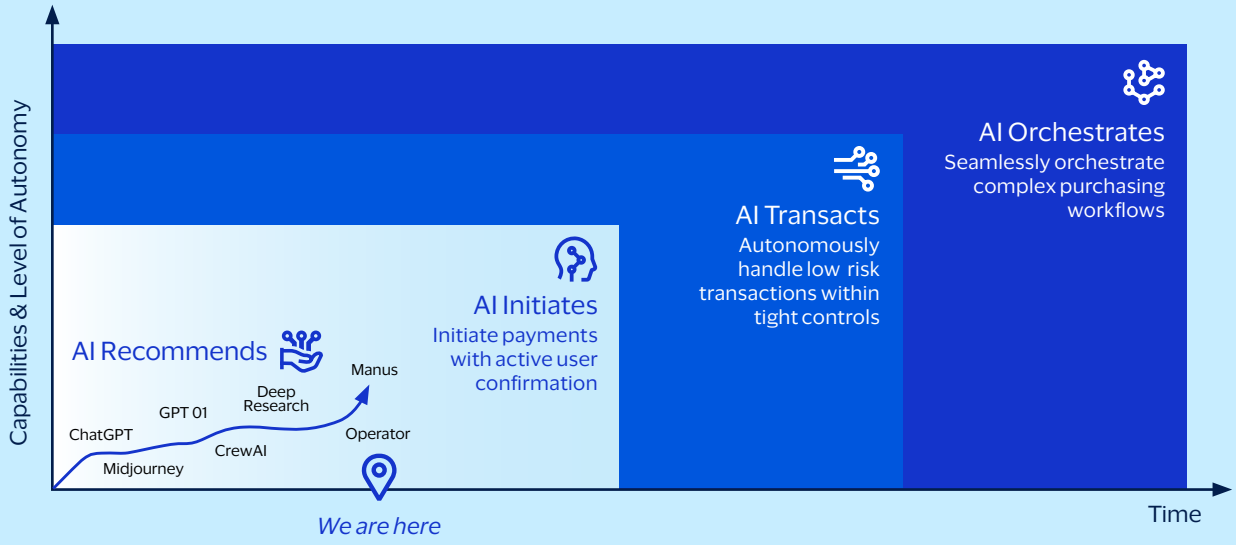
The next phase, AI Initiates, sees systems like OpenAI's Operator initiating checkout processes on a user's behalf. These fl ws still rely on user confirmation and authorisatio per transaction, with experimentation emerging but widespread deployment remaining limited. In this stage, human oversight remains essential.

In AI Transacts, agents could start to gain conditional autonomy – operating within narrow, predefined parameters to complete low-risk transactions end-to-end.

The final stage, AI Orchestrates, envisions agents managing complex purchasing workfl ws in real-time environments with minimal human input. This would represent a signifi ant shift in how digital commerce is structured.

By understanding these stages, we can better frame the challenges and opportunities ahead – as AI evolves from a helpful advisor toward a more autonomous assistant.

Evolution of agentic commerce



AI Recommends

In the current stage of AI-powered commerce, generative AI primarily supports human users as an intelligent advisor. These models can analyse inputs and generate text or audiovisual content, interacting with users across a range of channels – including chat interfaces, voice assistants and embedded tools.

At this stage, AI applications are not yet executing transactions. Instead, they provide purchase ideas, product comparisons or service suggestions based on prompts and user preferences. They could also act as personal optimisation assistants—helping users make smarter spending decisions, identify cost-effective merchants, or choose better delivery options. In our view, as these systems improve in reasoning and autonomy, they will become an entry point to initiate purchases and transact online.

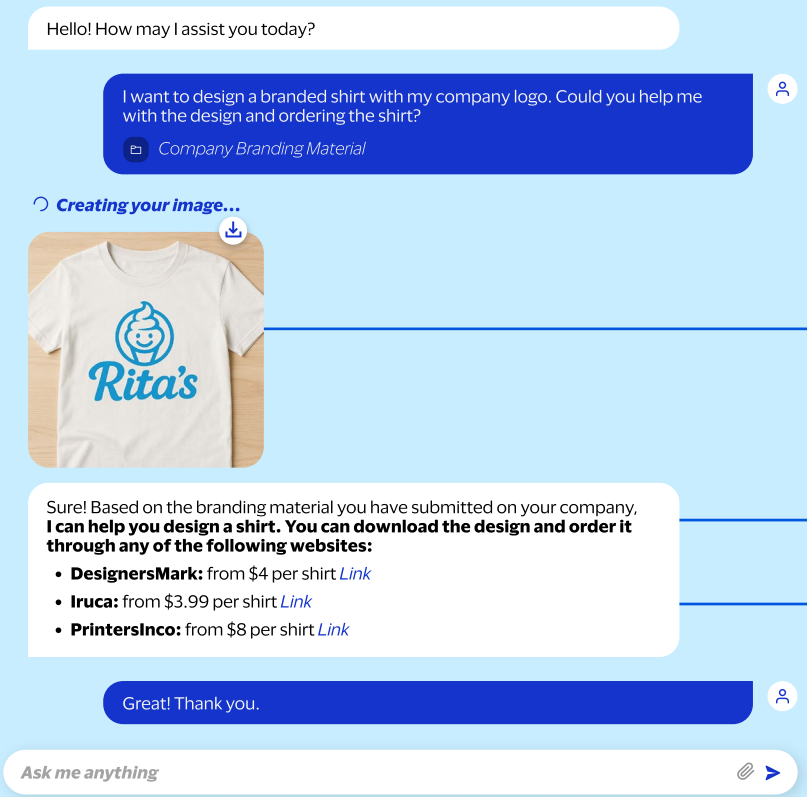
An example of this is Open AI's launch of shopping results through ChatGPT, which displays product carousels adapted to user requests – such as pricing – when mentioned in the prompt. Each product has a direct link to the merchant website, so it works as suggestions and requires users to continue their shopping outside ChatGPT[3].

66%
of consumers have used AI in the last 3 months[2]

92%
of those using AI for shopping like it and say it enhances their experience[1]

1200%
uplift in volume of internet traffic going from GenAI websites directly to merchant websites in 2024[1]

Mock-up of user using a Generative AI model to create a custom shirt ILLUSTRATIVE



1. Recommends without acting upon tasks
   — Can generate text, images and code
2. Zero-shot and reasoned answers with suggestions/ recommendations
3. Purchase recommendations

The scenarios depicted here are for illustrative and discussion purposes only, and do not represent any current or future products or services at Visa.

AI Agents: what they are and how they work

AI Agents are autonomous systems designed to process information, reason and take actions to achieve specifie goals. They integrate Large Language Models (LLMs) and contextual data, and can make use of external tools and APIs to function in a continuous loop of observation, decision-making and action.

This autonomy allows them to operate with minimal human intervention, adapting to dynamic conditions while pursuing targeted objectives.

AI agents are being developed to perform tasks in a wide array of domains such as coding (Cursor), browser use (OpenAI's Operator), legal (Harvey) or general-purpose computer use (Manus).

47%

of consumers are interested in using agents for commerce[4]

Agent-led use case examples

The opportunity for banks and payment companies is vast. As agent capabilities grow – automating complex processes, integrating with tools, and even collaborating with other agents – we expect to see rapid expansion in agent-led use cases across the ecosystem.

Sales Engagement Support

AI agents drafting proposals for prospective client outreach, based on company materials, real-time data and internal assets.

Real-Time Currency Exchange

AI agents autonomously performing currency conversion and executing international payments at the optimal exchange rates.

Predictive Cash Flow Management

AI agents autonomously predicting cash fl w needs and adapting budgets based on company activity.

Architecture of an agent

Drawing from Google and Anthropic's Agent definitions, the a chitecture of an agent typically has 3 foundational components:[5,6]

Memory

Short-term memory allows the agent to retain recent information within current interactions with the user (user inputs, immediate results, interaction history...) to maintain continuity and coherence. Long-term memory builds on this, enabling the agent to store and recall persistent knowledge across other interactions with a user (user preferences, past behaviour, contextual data...).

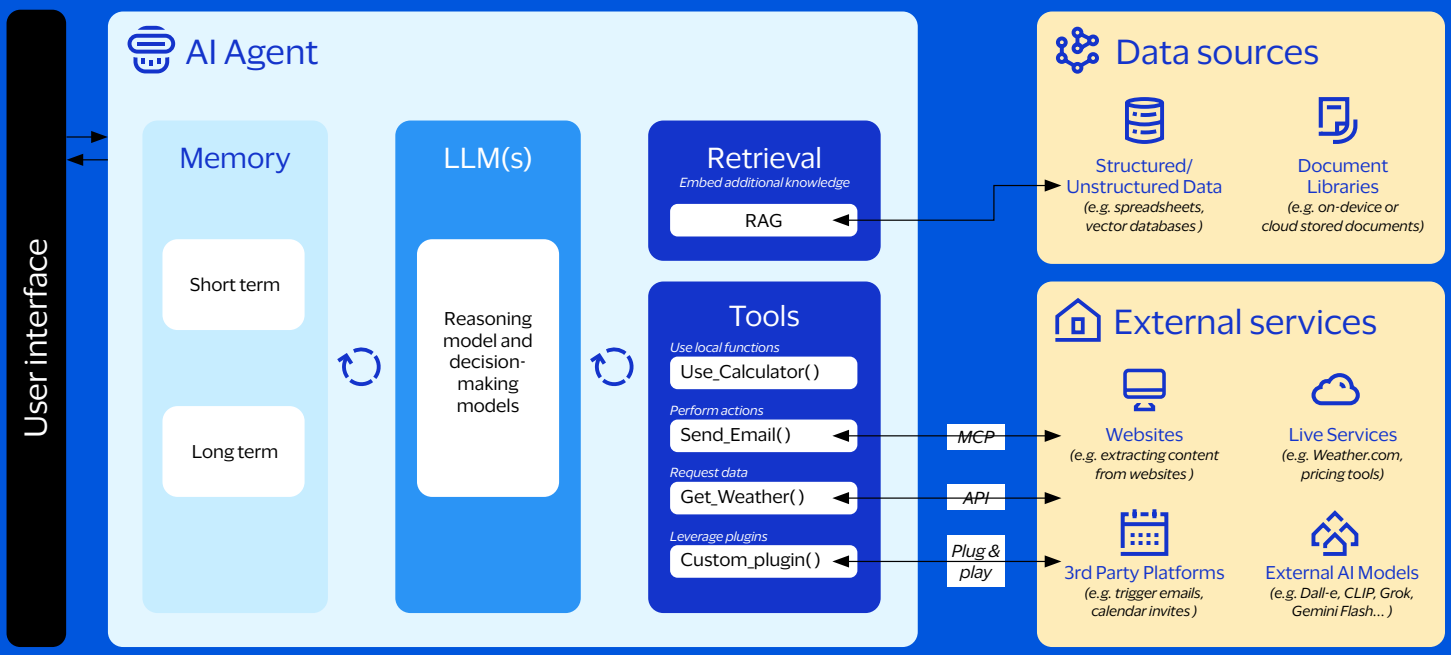
Models

The agent uses one or more language models for decision making and is trained to understand prompts based on reasoning frameworks (e.g. ReAct, Chain-of-Thought or Tree-of-Thought).

Tools

Tools enable agents to extend their capabilities beyond the LLM's reasoning. They allow agents to retrieve information, interact with external systems, or perform actions. Tools may connect to data sources, external platforms or local functions.

Simplified AI Agent a chitecture ILLUSTRATIVE



As agentic workfl ws gain momentum, companies are introducing new standards and solutions to support agent development. Anthropic's Model Context Protocol[7] (MCP), for instance, helps developers build agents by offering pre-integrated access to data and tools – eliminating the need to connect to each service individually. Other emerging frameworks include LangGraph, CrewAI, and OpenAI's Agents SDK, although many more are appearing weekly.

AI Initiates

As we increasingly enter the AI Initiates phase, we begin to see agents not only advising users but also taking action to initiate payments. In this stage, AI tools can interact with eCommerce platforms, with the potential to initiate checkout journeys – though final confirmation and authorisation could remain with the user on a one-by-one basis.

Leading AI Labs and open-source solutions are releasing research previews or beta versions of agents capable of executing tasks on behalf of the user by simulating human browsing behaviours. While early iterations of these agents are still limited in terms of reliability and consistency, they mark a critical transition toward AI-initiated payments.

In parallel, we're seeing AI applications explore third-party integrations with plugins, extensions and APIs. This has the potential to shape the first wave of Agentic Commerce.

In this section, we offer a view on online transaction journeys, powered by AI applications. We consider all three models are, at least technically, plausible with today's payment infrastructure.

Some of the early AI-initiated payment journeys

A. Browser-automation agents | B. Integrated tools and extensions | C. AI platform as wallet and payment aggregator

A. Browser-automation agents

How do they work?

Browser agents work by processing natural language prompts, breaking them into actionable steps and executing those actions in a web browser. Generally, they capture and interpret screenshots to identify layout, elements and click targets – then simulate human-like interaction using a keyboard and mouse. Since websites are built for human users, this method allows agents to browse and transact without direct APIs, navigating interfaces as a person would. It means they can navigate standard e-commerce flows and go up to the online merchant's checkout processes, without human interaction.

Live examples of this are OpenAI's Operator, Claude Computer Use, Amazon's Nova Act and solutions like Manus which work in conjunction with cutting-edge LLMs.

Making progress

While the potential of AI agents is significant, their current capabilities remain limited. Many still rely on clunky workarounds like web scraping, often stalling or failing on complex websites. In theory, they would be able to automate part of the checkout process, but would still rely on human intervention to input data such as payment credentials.

As the checkout process is carried out on a standard web browser, customer authentication processes (if required), would likely follow the same standards and logic as in today's flows. (e.g. in-app SCA via a banking app). However, browser automation may raise privacy, legal and compliance risks.

Regulatory consideration

As browser agents evolve, regulatory compliance and security must remain a core design consideration. Under data protection laws like GDPR, any personal data collected – including during website scraping, typically used by browser agents – requires a clear legal basis. Agents may also trigger cookies or tracking technologies while mimicking user interactions, raising consent requirements under regulations like the ePrivacy Directive

Additionally, some jurisdictions mandate direct user acceptance of terms and conditions, which could pose challenges when agents act on behalf of users [8].

Mock-up of an e-commerce payments form through a "computer-use" type agent (1 of 2) ILLUSTRATIVE

Hello! How may I assist you today?

I want to buy The Orchard Beyond the Lake hard cover limited edition book on the Marketplace. It must have at least a 4-star rating and cost between $10-40.

I could not find the hardcover copy of The Orchard Beyond the Lake with your rating and cost specifications.

Would you like to switch to a paperback edition?

1 Adapts when needed and asks clarifying questions

Yes, that is fine.

I found a book that fits your requests. Please confirm if you would like to **proceed to checkout** or if you would like me to keep searching.

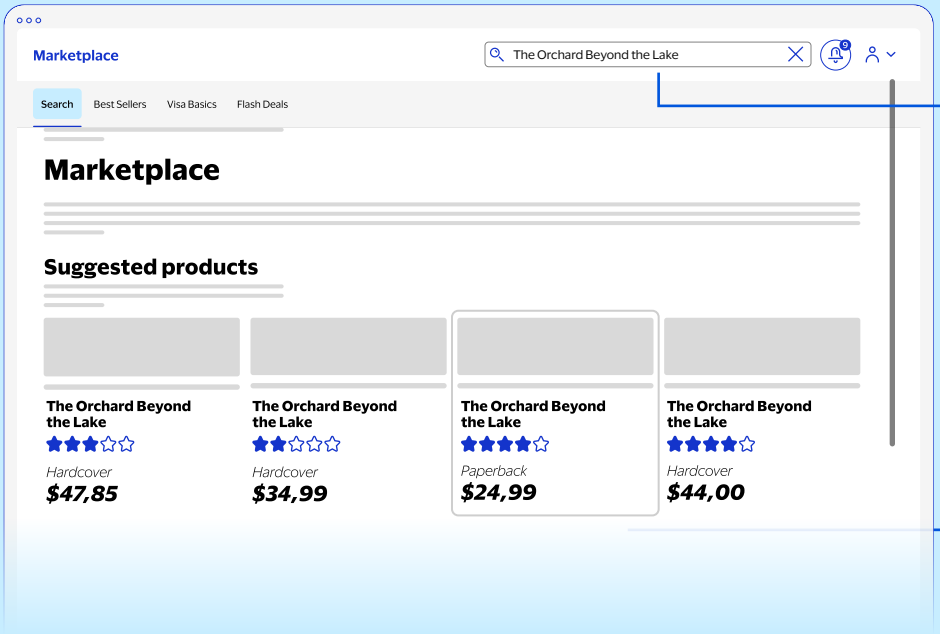
2 Checks before proceeding to checkout

Continue to checkout.

You are now in private mode. Follow the steps of Operator and provide input if required.

3 Hands over checkout process to user

Ask me anything



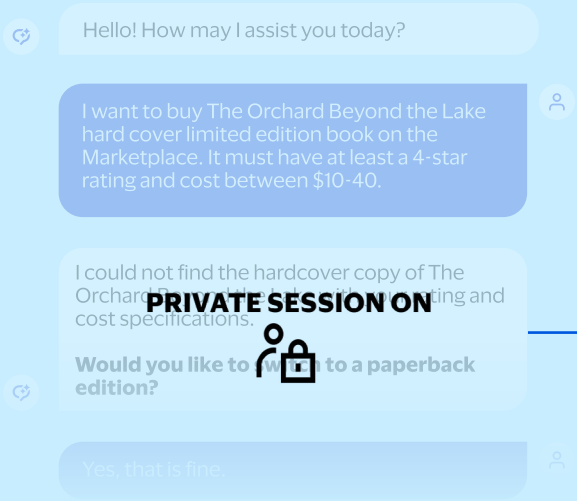
Agent interacting

Browser agents can type in search bars and navigate websites, mimicking user activity

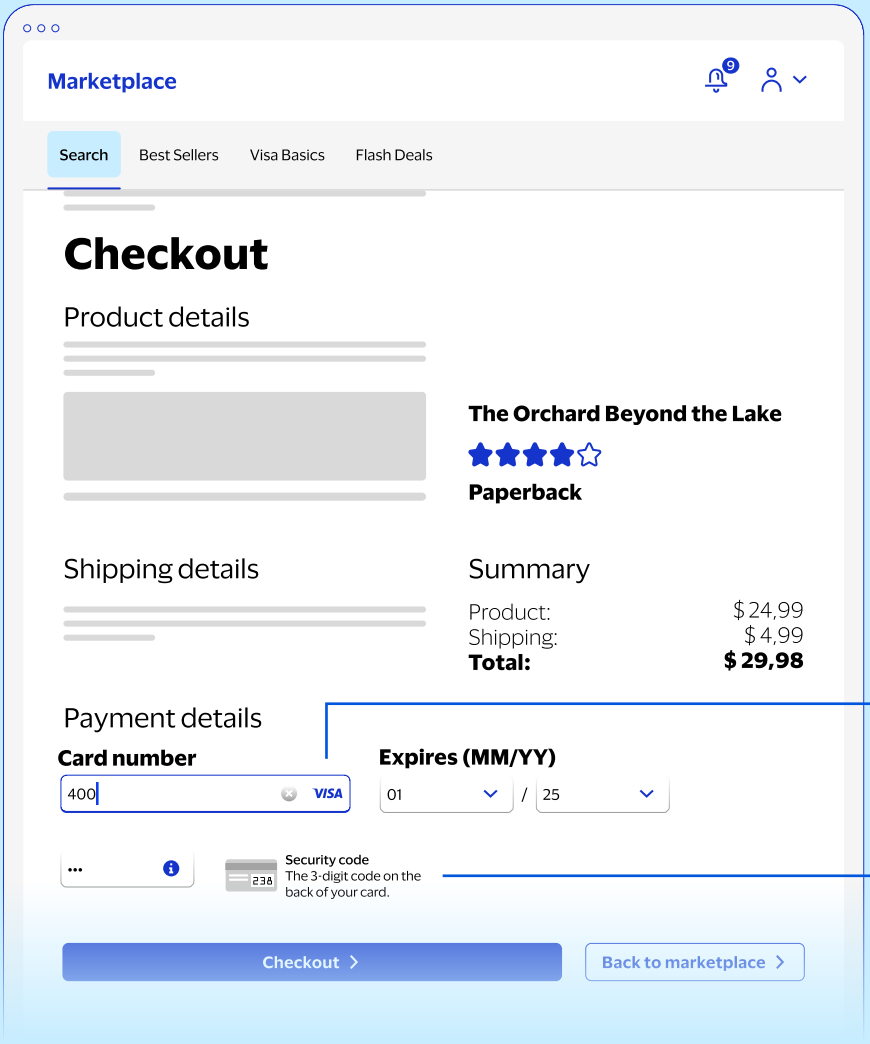
Agent uses mouse and keyboard to interact with websites

The scenarios depicted here are for illustrative and discussion purposes only, and do not represent any current or future products or services at Visa.

Mock-up of an e-commerce payments form through a "computer-use" type agent (2 of 2) ILLUSTRATIVE



1 Private session means the user takes over and agent cannot see information inputted



User interacting

User manually enters payment information

2 Users go through the normal checkout process

The scenarios depicted here are for illustrative and discussion purposes only, and do not represent any current or future products or services at Visa.

B. Integrated tools and extensions

AI model developers and consumer-facing applications have begun integrating external tools into their workfl ws – often via plugins, extensions, GPTs with external actions, or artifacts. These early integrations mark a shift toward agents functioning not just as responders, but as coordinators of multi-step user journeys.

If this trend continues, we could see workfl ws where an AI assistant compiles a grocery list tailored to a user's health needs, preferences, and budget – and then places the order using an integration with a grocery delivery service.

Three potential use cases

In travel, we could search for and book fli hts using tools like Google Flights plugins.

For SMEs, agents embedded in ERP or accounting platforms could identify pending invoices and use supplier integration to pay with stored credentials.

For bookings, users could check availability, make a reservation and confirm payment th ough a merchant add-on.

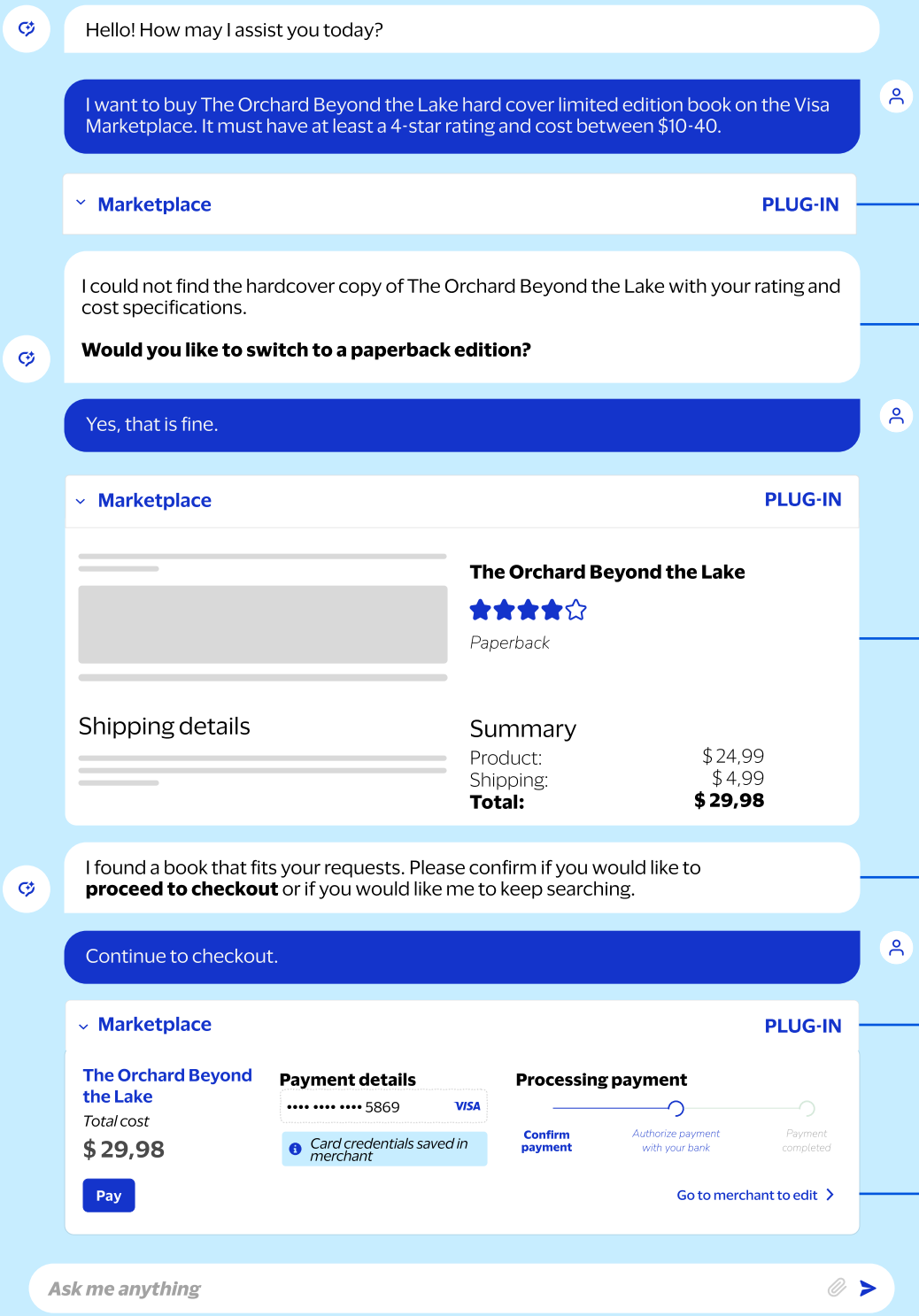
We believe that, in these early cases, the most flexible payment workfl w will consist of using the payment acceptance capabilities of the tool or software provider. This includes, for example, a card/token on file sto ed as a payment credential. The agents may act as intermediaries, connecting the user's purchase intent with the merchant's payment processing capability, without directly handling transactions.

The integrated plugin or action might request a confirmation within the AI tool while p oviding the necessary details for the user to correctly identify – and potentially add or modify – the payment credential stored by the service provider.

In this case, it would be the tool or software provider's PSP – the one handling the transaction processing and authorisation request, thus requiring minimal changes to existing infrastructure, except for cases where strong customer authentication may be required.

Agents under this paradigm rely on merchants having secure and functional payment processing infrastructure, which the agents could trigger (e.g., via an API call). The success of this model depends on merchants' willingness and ability to develop and maintain these integrations. Where integrations are missing or inconsistent, it could lead to conflicting user experien e across different merchants.

Mock-up of user purchasing a book through an integrated tool ILLUSTRATIVE



1. Request is directly handled on chat, through API or Plug-In
2. Agent adapts, pulling information from plug-in
3. Pulls product information from merchant
4. User does a final check and pays within AI platform interface
5. Pulls cards information from merchant, leveraging COF capabilities
6. Payment is sent to merchant and processed with their payment capabilities

The scenarios depicted here are for illustrative and discussion purposes only, and do not represent any current or future products or services at Visa.

C. AI platform as wallet and payment aggregator

The third model positions the AI application whether general-purpose or verticalised – as both a wallet for the user's payment credentials (e.g. card-on-file, tokens, tokenized accounts) and an orchestrator of downstream payments to the merchant.

In this setup, the AI platform may:

1. Receive payments from users or customers
2. Execute and manage payments to third-party providers, including usage-based services, merchants, marketplaces, paywalled content providers or even other agents

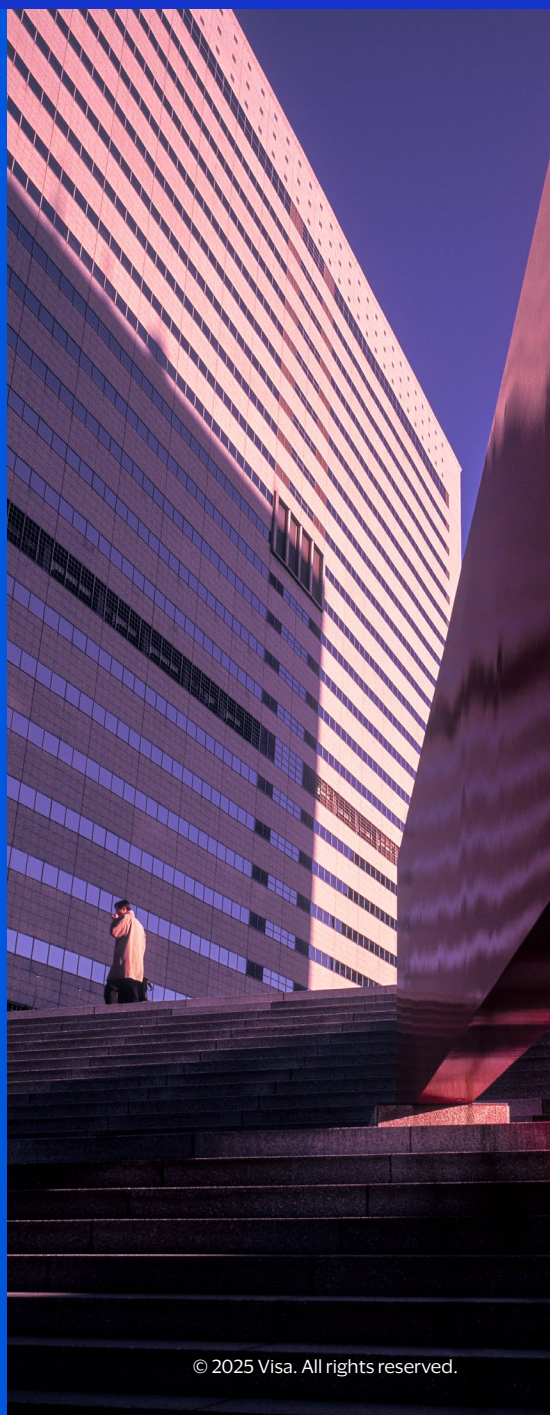
This approach is inspired by models long used by online aggregators such as marketplaces, online travel agencies (OTAs) or food delivery platforms. These companies offer users a single, consistent payment experience while managing onward payments to a diverse set of suppliers and services, in a second B2B transaction, following the staged wallet model.

An early example of this model on AI is Perplexity's 'Shop like a Pro' solution[9]:

- Perplexity Pro users in the US can research, compare and purchase products directly in the app.
- The AI aggregates product information from platforms like Shopify and displays prices, product characteristics, reviews and features in real time.
- Users complete checkout via a 'Buy with Pro' button, without leaving the interface.
- Perplexity receives payment from the user, then initiates a separate payment to the merchant.

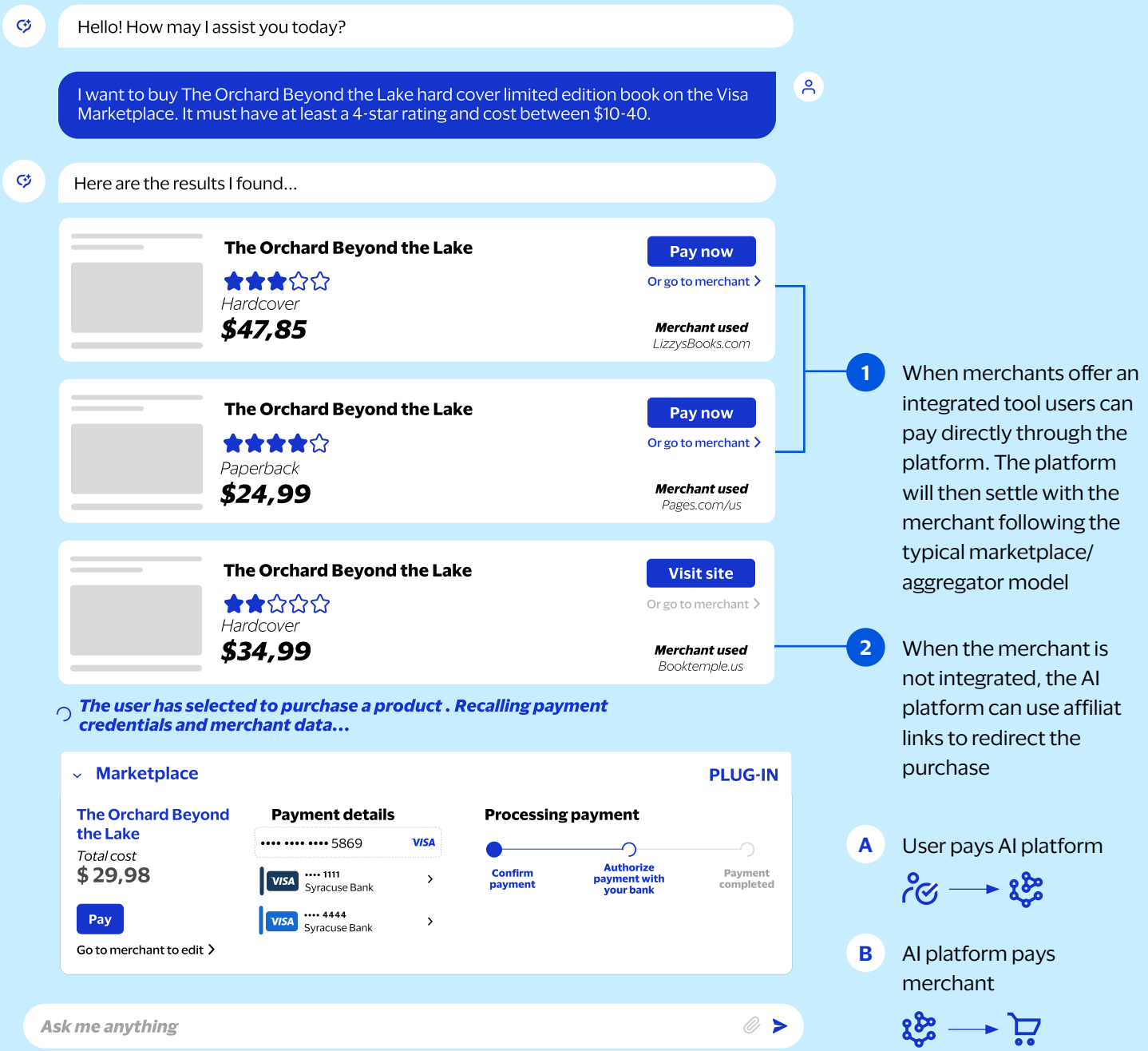
For this to work, AI apps must securely store and manage user payment credentials, trigger payment execution through specialised PSPs, and route funds to third parties using methods such as:

- Closed-loop payment systems.
- B2B virtual cards and tokens.
- Domestic/regional transfer schemes (e.g. ACH, SEPA).
- Push-to-card, account or wallet networks (e.g. Visa Direct).



(Place holder for legal caveat)

Mock-up of a general-purpose application payments wallet ILLUSTRATIVE



1 When merchants offer an integrated tool users can pay directly through the platform. The platform will then settle with the merchant following the typical marketplace/ aggregator model

2 When the merchant is not integrated, the AI platform can use affiliat links to redirect the purchase

A User pays AI platform

B AI platform pays merchant

The scenarios depicted here are for illustrative and discussion purposes only, and do not represent any current or future products or services at Visa.

AI Transacts

The AI Transacts phase introduces - limited but increasing – autonomy when operating. At this stage, AI agents are entrusted with the authority to autonomously complete low-risk, potentially low-value transactions for users. Autonomy, however, falls under a spectrum.

We believe that agents may increasingly earn greater autonomy in executing sensitive tasks, such as authorising payments without human intervention, once they consistently prove their reliability in lower-risk scenarios.

The first instan es of AI-executed payments may have to be undertaken on very controlled settings, with AI-powered software and agents being able to purchase on users' behalf and execute payments for low-risk transactions. Payers will need to proactively accept - and potentially authenticate - payments for higher amounts, outside the established parameters or for transactions that don't fall under the low-risk category.

These controls might include:

- Spend thresholds (e.g., up to £30 per transaction or £100 total daily spend).
- Velocity checks (e.g., a maximum of 5 transactions per run).
- Whitelisted services, merchants, apps or APIs that the agent is authorised to use (vetted by the agent provider and/or the user).

In this phase, we will potentially see the transition towards a pass-through payment model, instead of the staged wallet of the previous phases.

Visa Intelligent Commerce's (VIC)* Payment Instructions API will execute payment controls to validate that AI agent payment actions are aligned with user intent.

Workfl w and agent parametrisation: permissions and controls

1 Before starting the task, the user could set transaction-related permissions and controls. After prompting the agent for the requested goal, the AI agent could reason and present a comprehensive execution plan for user validation.

2 This plan would outline projected steps and – potentially – allocate funds or tokenize a credential for payments. We imagine it as a detailed breakdown of how the task will be accomplished, any potential issues that might arise and how resources, particularly financial resources, will be used.

3 The user retains control by reviewing, modifying and approving the AI agent's proposed plan, ensuring alignment with their objectives.

Transactions that fall within the defined limits and boundaries could be performed by the agent autonomously. Transactions exceeding these limits would require pending customer confirmation to p oceed.

*For additional details, refer to the closing sidebar "Visa Intelligent Commerce – Visa Product Drop April 2025"

Such rules could be implemented at two levels

Workfl w-based policies

Defined by the user be ore each agent execution

A workfl w refers to any time the agent is prompted to perform a new task – from planning a trip to processing an order. Workfl w-based policies allow users to set task-specific ontrols at this point, emphasizing trust and transparency. This approach also encapsulates risk by validating actions before each execution.

Agent or profile-l vel permissions

Persistent settings and controls applied across all agent activities

Permissions can be defined at the agent or user p ofile level, applying across all workfl ws moving forward. This is useful for agents performing repeated tasks or consistent requests.

- Limits set at the agent level apply to all transactions that agent handles.
- Limits set at the profile l vel apply across all agents used by the user on that platform.

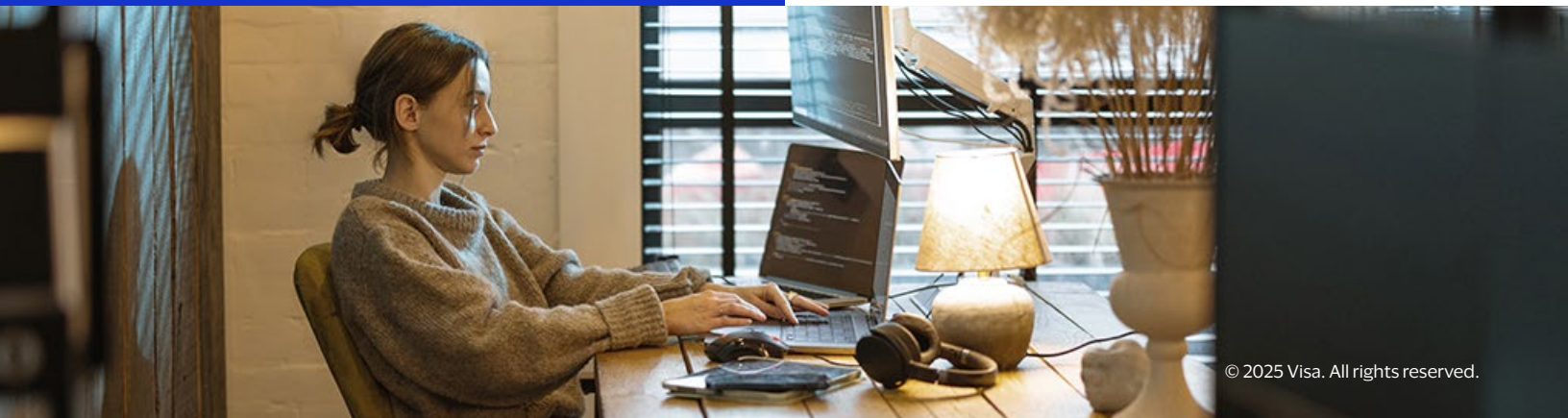
Visa expects both models to coexist. Workfl w-based control may be preferred for ad hoc or complex tasks, while profile-based settings will suit epeat transactions and consistent use cases.

Some transaction controls may be configu ed and stored directly within the agent or local software, while others may remain embedded at the credential level—tied to the token associated with a specific device-agent pairing, as seen in Visa Intelligent Commerce (VIC).

Frameworks like VIC or emerging agent SDKs, like Stripe's, are already supporting these models, using API keys to let developers and users define the specific API alls the agents are permitted to make.

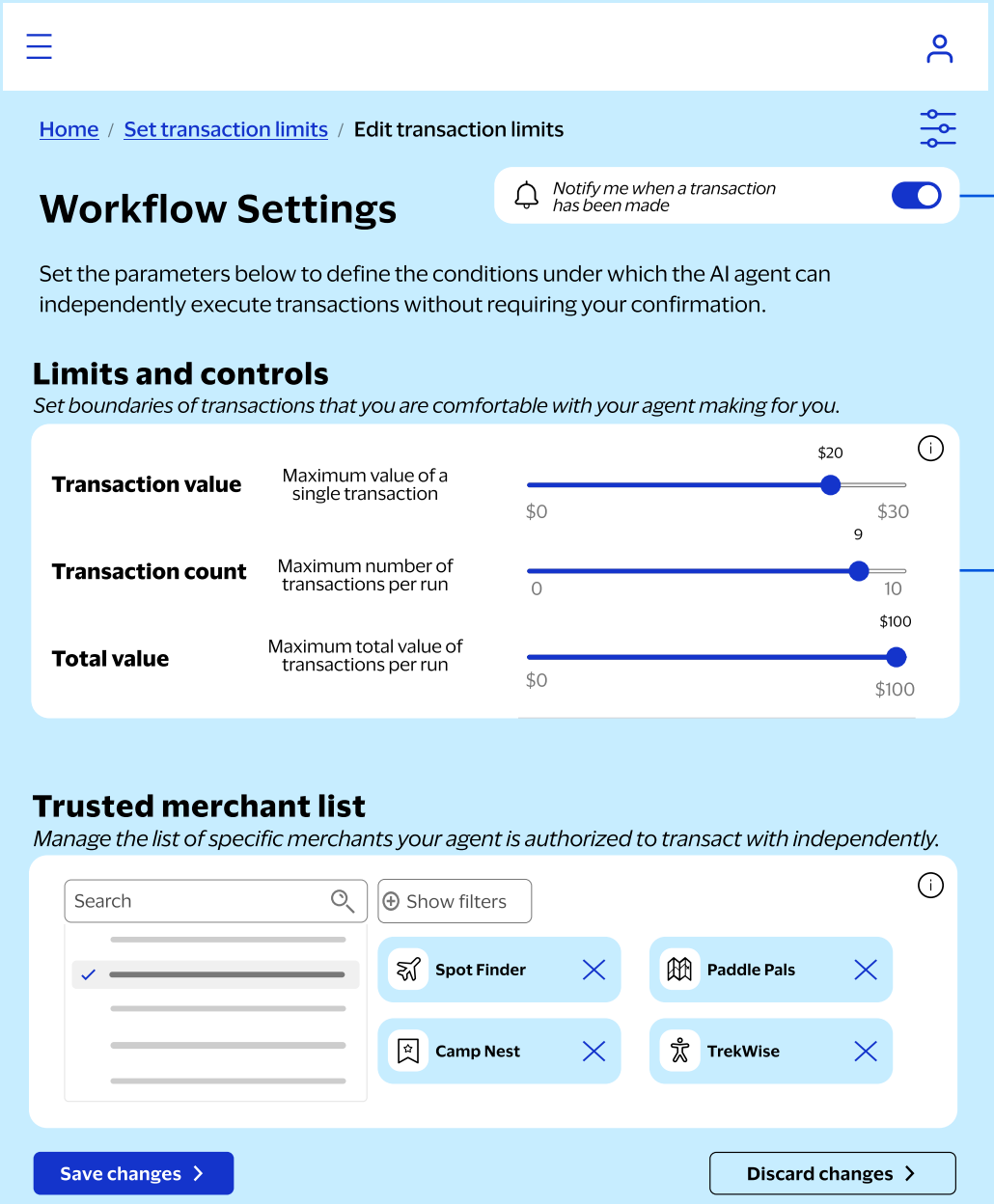
For example, developers can set up the APIs to generate single-use virtual cards with custom spend limits, merchant restrictions and transaction criteria, enabling a payment from the agent to the merchant. This can be parametrised on a per transaction basis.

Stripe's SDKs also support a human-in-the-loop approval process, allowing users to authorise transactions in real time. Before the agent finalises a purchase, the intended transaction can be presented to the user (within the agent platform) for explicit approval[11]. At this stage, agents would be able to autonomously complete payments with strict parameters and controls in place, along with user confirmation when ne essary. In AI Transacts, friction would be reduced in transactions within the parameters while maintaining oversight and trust in more complex payments.



Mock-up of the workfl w-specific settings and ontrols for an AI-powered travel agent ILLUSTRATIVE

A First, the user sets workfl w settings under which the AI agent can transact...



1 User would set transaction parameters for the workfl w

2 Users can choose what transactions would be completed by the agent

The scenarios depicted here are for illustrative and discussion purposes only, and do not represent any current or future products or services at Visa.

Simplified user experien e of the AI Agent execution of tasks ILLUSTRATIVE

B … the agent then proceeds to execute within the parameters

Transaction settings for agent-executable spend

Maximum transaction value	Maximum number of transactions	Total maximum spend	
$20	*9 transactions*	*$100*	Edit ›

Hello! How may I assist you today?

I'm planning a trip to Colorado from July 10 to July 17. I've got a total budget of $1,300. I'd like medium-level accommodations, want to do kayaking, hiking, and check out some museums. Also, I definitely don't want to miss camping at Maroon Bells and Great Sand Dunes.

Sounds like an amazing trip! Thanks for setting those clear parameters. Based on your total trip budget of $1,300, here's my suggested plan:

Category	Description	Budget allocated
Accomodation	Medium-level hotel/cabins (5 nights)	**$455** *(35%)*
Camping	Campground reservations (2 sites)	**$195** *(15%)*
Activities	Kayaking, guided hikes, museums	**$390** *(30%)*
Local Transit	Rental car + gas	**$195** *(15%)*
Food & Supplies	Trail snacks, basic groceries, water	**$65** *(5%)*
Total		**$1,300**

I'll manage your agent-executable spend with small-value bookings (kayaks, hikes, museums, etc.), and keep bigger-ticket items (campgrounds, accommodations) on hold for your approval. **Would you like to proceed with this resource allocation?**

Yes, that looks good. Go ahead.

Awesome! I'm going to begin planning and booking, starting with your activities and museum visits. I'll keep you updated and flag anything that requires your approval.

Planning and executing…

#	Item	Cost	Status
1	Kayaking Grand Sand Dunes	**$14**	Completed
2	Trail pass – Garden of the Gods hike	**$8**	Completed
3	Guided hike – Hanging Lake	**$19**	Completed
4	Camping – Great Sand Dunes (2 nights)	**$43**	Pending review Approve ›
5	Cabins – Maroon Bells (2 nights)	**$185**	Pending review Approve ›
…		…	…

Agent Spend Summary
Executed Transactions (3/9 used): $41
Pending Transactions (On Hold): $228
Total Agent Budget Spent or Committed: $41 / $100
Remaining Agent Capacity:
- $59 available
- 6 execution slots left

Ask me anything

Workfl w Settings

Transaction settings previously established will be applied

OR

Account Settings

Maximum transaction value
$20

Maximum number of transactions
9 transactions

Total maximum spend
$100

1 Agent presents a comprehensive execution plan for user validation

2 Resource allocation is confirmed or pre-execution validation

3 Transactions are completed or left on hold depending on transaction parameters

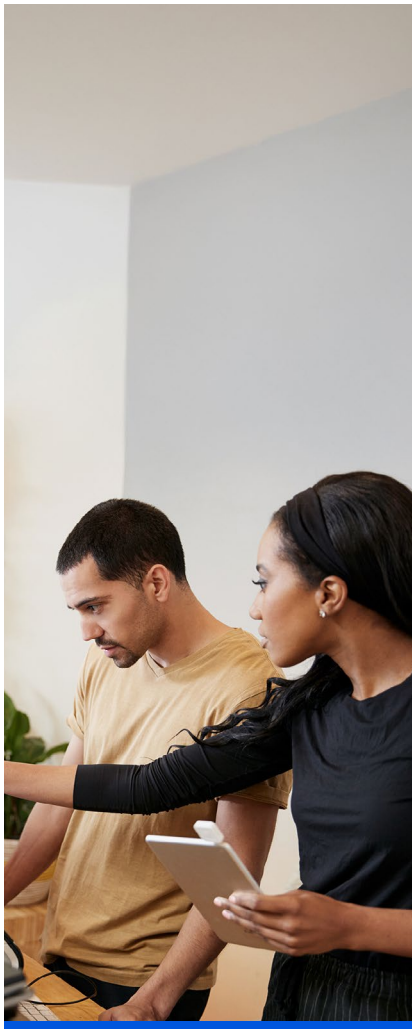
The scenarios depicted here are for illustrative and discussion purposes only, and do not represent any current or future products or services at Visa.

AI Orchestrates

The next frontier in our framework – AI Orchestrates – envisions advanced agents managing complex workfl ws. Here, AI agents would go beyond initiating and completing discrete tasks and could plan, execute and iterate over complex processes with minimal human input.

In this stage, it's possible to envision a plethora of potential use cases for businesses and consumers, including:

- A travel agent that plans and makes bookings for a bespoke trip to Japan for two people, comparing providers and optimising price and value.
- A personal-shopping agent that scans product rating websites to purchase a pair of training shoes from the best-value online marketplace.
- AI-powered 3D design software that autonomously purchases 3D assets from different online marketplaces to achieve a desired result.
- A marketing agent that dynamically monitors keyword pricing to purchase ad campaigns in several sites and search engines.
- A logistics agent that schedules vehicle maintenance, arranges payments to the auto repair shop and ensures minimal downtime in the fleet's schedule
- A deep research agent that sources information paying for access to premium data APIs to complete an insights brief.



These examples illustrate the emerging versatility of AI agents, from the more tangible and realistic to the more forward looking and futuristic.

Developing general-purpose agents with high autonomy is complex. These advanced agents might operate with mid to high levels of autonomy, would have the ability to execute payments while requiring continuous automated monitoring and audit mechanisms. Different levels of intelligence, autonomy, reliability and trust will be required to ensure actions align to human intention. To support this, technical, regulatory, compliance and risk frameworks should ideally evolve in parallel.

Based on today's primitives, AI agents would need three elements to manage payments:

A. An assigned budget

B. Access to payment credentials

C. Agent identifi ation for secure authentication

A. An assigned budget

Agents may require a pre-defined budget, set by the use , to complete a given task or group of tasks. This budget could be provisioned through:

- Permissioned access to a pre-funded wallet (owned by either the agent or the AI platform).
- A tokenized payment credential.

Regardless of the model, agents would still require a well-defined f amework and scope of action to manage the budget effectively. While these parameters will be more permissive compared to the AI Transacts phase, they remain essential to ensure that the agent's actions are aligned with human intentions.

Risk and liability frameworks will still need to be in place to mitigate certain risks like overspending, malicious intent or fraudulent transactions.

Nearly

50%

of Visa's digital transactions are tokenized today[1]

1bn

tokens added just in the last quarter[1]

B. Access to payment credentials

Payment credentials could be stored within the agent's own wallet or linked to the user's payment instruments. When payment credentials are tied to the user's instruments, stringent security measures must take place to protect sensitive information and prevent unauthorised use.

Management of payment credentials should be flexible, all wing for updates, revocations and reactivation. This ensures that the AI agent's ability to execute payments remains secure and adaptable to changing circumstances. However, as agents expand across apps, wallets, and operating systems, there may be a growing need for users to regain visibility and control over where and how their credentials are stored and used.

Visa Intelligent Commerce would include a tokenization service that is designed to grant access to the user's payment credentials via agent-requested tokenized digital credentials.

C. Agent identifi ation for secure authentication

Most authentication systems today assume that a human is present behind the screen. As agents begin to initiate and execute payments independently, the model needs to transition from proving you are the right human to proving you are the authorised agent on behalf of the right human[12].

To prove agent identifi ation, we envision agents using unique identifiers within digital e osystems linking them to a specific plat orm, organisation or individual. These identifiers an be:

- A unique and cryptographically secure ID credential for an AI solution or individual agent that is linked to its set of permissions.
- An unambiguous and revocable link with the associated user or company.

We foresee that current regulatory initiatives on Digital Identity across different markets may need to evolve to incorporate agent authentication frameworks within their scope.

The previously mentioned Visa Intelligent Commerce's payment tokens are bound to user devices and secured using Passkeys, ensuring that all user instructions to the agent are verified. hese tokenized digital credentials confirm that a onsumer's selected agent is allowed to act on a consumer's behalf, bringing identity verifi ation to AI-driven commerce.

Striking the right balance between AI autonomy and human-in-the-loop journeys will be critical to ensure trust in agent-led payment fl ws. Human intervention and fallback mechanisms will still be necessary – particularly for high-value transactions, risk-prone use cases or when regulatory thresholds (e.g. PSD2 SCA) are triggered.

Liability rules will also need to adapt to reflect these new dynamics, ensuring clarity around responsibility and recourse when agents act independently. In this context, Visa is actively collaborating with industry participants, including issuers, acquirers, PSPs, merchants and AI platforms, to establish suitable liability frameworks.

Receiving and managing funds

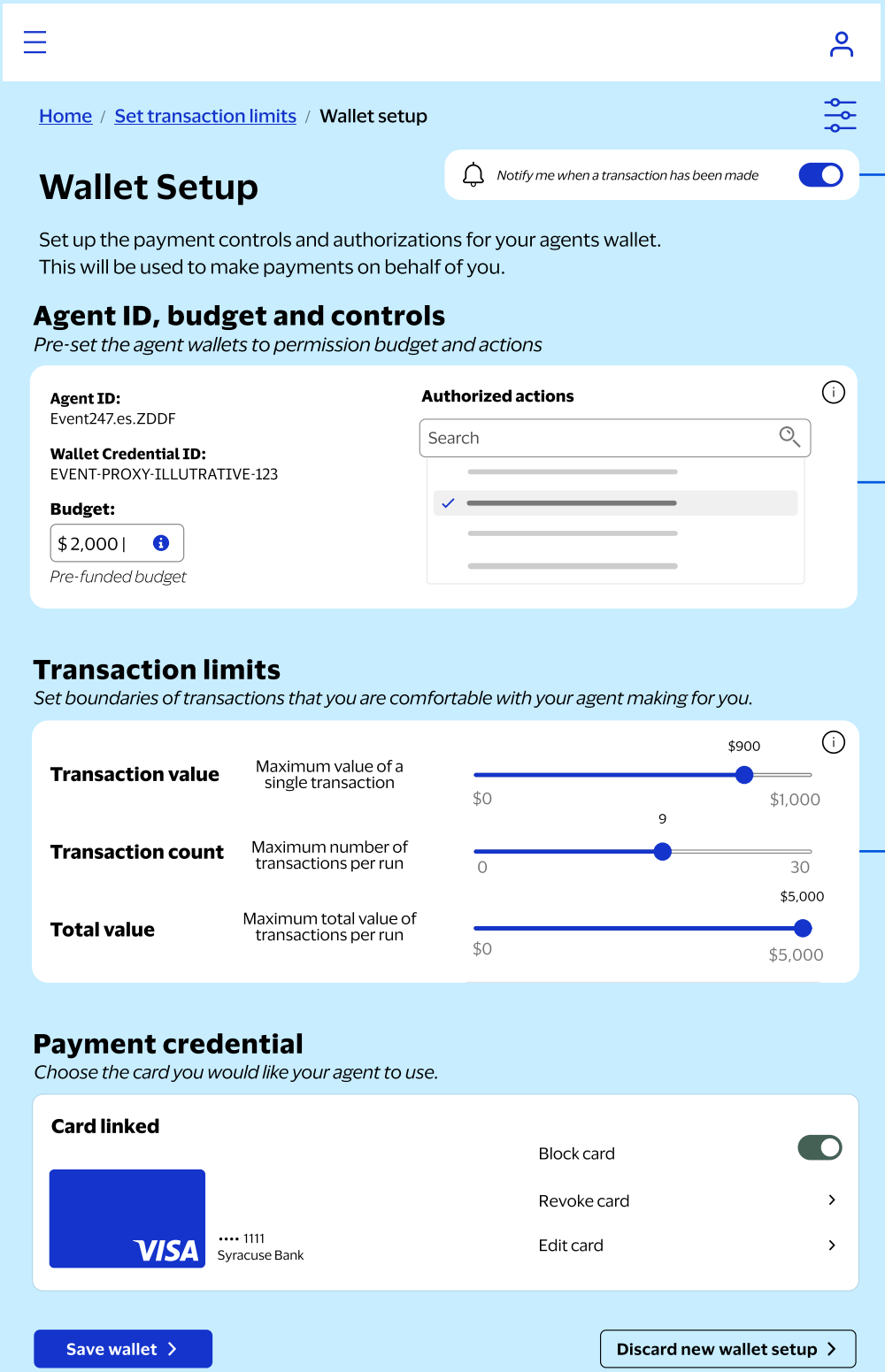
In the future, we might see AI agents evolving to comprehensive roles within digital environments. This signifies a shift f om task-oriented to role-oriented AI, where agents manage ongoing responsibilities and interactions.

For example:

- Autonomous Customer Success: An AI agent managing customer relationships using defined objective metrics (e.g. satisfaction, retention). It would have a budget to offer discounts, issue refunds or upgrade users to premium services.
- Dynamic Supply Chain Management: An AI agent managing a company's inventory and supply chain, negotiating with suppliers, placing orders and executing payments, optimising for cost, timing and efficie y. The agent would pay for raw materials, shipping and storage, dynamically adjusting its strategy based on real-time market data.

For this vision to scale, foundational systems must support agentic activity natively – not as an edge case, but as a core feature of digital commerce.

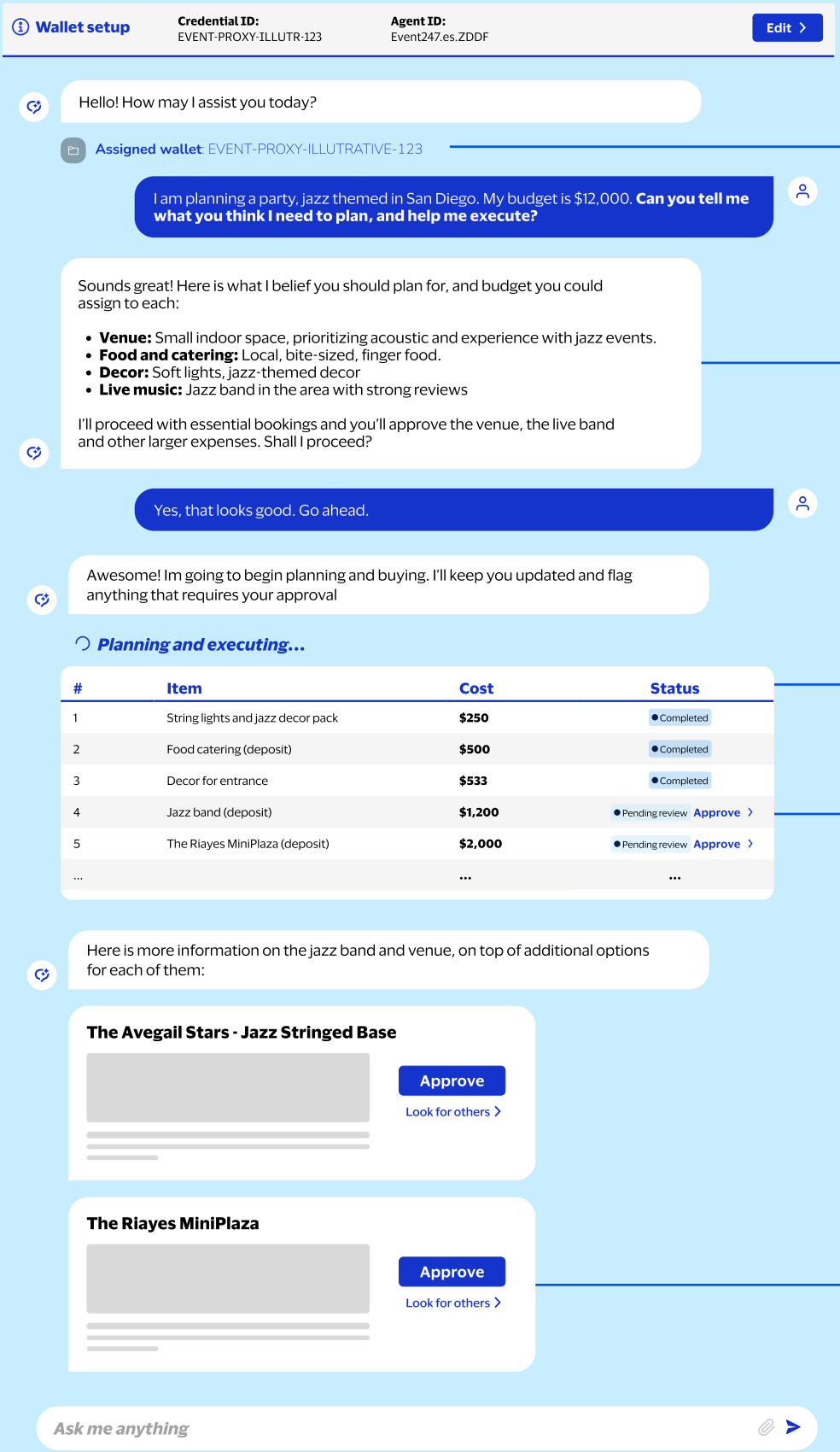
Mock-up of the settings and parameters for an Agent Wallet ILLUSTRATIVE



1. Agents have a wallet with an ID linked to the parameters and authorizations
2. Agents would have identifiers associated and pre-funded budget
3. Transaction parameters would also be needed

The scenarios depicted here are for illustrative and discussion purposes only, and do not represent any current or future products or services at Visa.

Simplified user experien e of the AI agent managing tasks ILLUSTRATIVE



1 Users will be able to choose from different pre-set wallets

2 Validation of the execution plan can help align user expectations

3 Transactions automatically completed within the parameters

Payment execution

Agent ID: Event247.es.ZDDF
Wallet Credential ID: EVENT-PROXY-ILLUTR-123
Authorization:
Credential ID: EVENT-PROXY-ILLUTR-123
Actions Authorized: ["Decor", "Amount<=$900", "Platform=Marketplace"]
Authenticated by: User3349283
Transaction Status: Confirmed

The payment execution is a transparent process, with all relevant information available to the user

4 Additional information and options are displayed for transactions that exceed the established parameters

The scenarios depicted here are for illustrative and discussion purposes only, and do not represent any current or future products or services at Visa.

> We are witnessing the emergence of autonomous agents capable of completing end-to-end transactions—from discovery to checkout—within the guardrails of stored credentials and user-defined limits

> As these agents grow more intelligent and context-aware, their impact on customer experience will deepen, reshaping expectations around trust, identity, and protection. This shift marks the beginning of a new era in commerce—beyond social—where AI becomes not just a tool, but a trusted actor in the customer journey.

Alicia Ngomo
Global AI Practice Lead, VCA

Visa Intelligent Commerce

Product Drop April 2025

Visa Intelligent Commerce consists of a partner program and advanced suite of integrated APIs and enhancements, built to support AI Commerce and deliver ideal customer experience in a secure, transparent manner.

Partner Program

Commercial program for AI platforms, Agents and their developers to onboard and deploy Visa's AI Commerce capabilities safely and at scale.

Components:

Designated agent: Know Your Agent (KYA) in development to help ensure Agent can comply with PCI standards and Visa data protection policy.

Agent onboarding: Agent needs to register for access to transact in Visa ecosystem.

Purchase protections: Exploring Visa Rules updates to address role of Agents.

At Visa we believe the payment industry benefits by g owing the ecosystem. AI agents are the new frontier, and we are poised to grow with them.

Agent APIs

5 AI Commerce services to enable network-level authentication, personalization and interoperable Visa payment experiences.

Tokenization: Enable agent to request tokenized credentials that are bound to that agent.

Authentication: Ensure agent performs user authentication during token provisioning request and before transacting.

Payment Instructions: execute payment controls to validate that AI agent payment actions are aligned with user intent.

Signals: Validate transaction data received from agent against consumer intent to help manage disputes and prevent fraud.

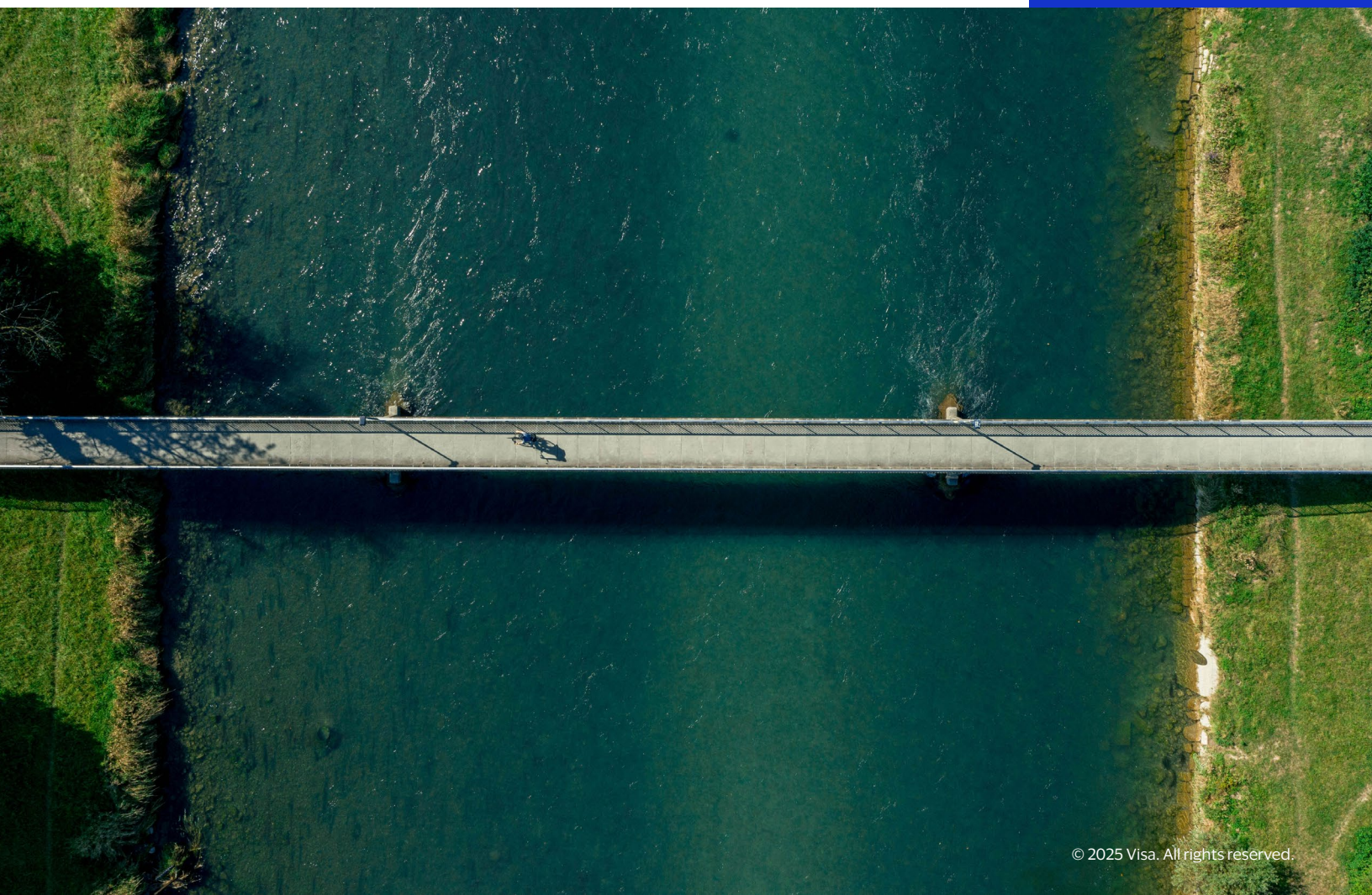
Personalization: With user consent, provide agents insights on user card behavior to enable more personalized experiences.

The Road Ahead

While the future of autonomous commerce and evolution towards agentic payments provides an exciting picture, the reader might have realized that several adaptations and developments are required to materialize it effectively. For example, eCommerce retailers that have focused on optimising the online checkout experience and invested in their digital acquisition channels (through SEO, paid advertising and organic media) will probably need to rethink how to best place their brands on an Agent as personal shopper era.

Most current payment experiences, risk controls, legal frameworks and user interfaces have been built around the assumption of a human in the loop. In an AI-led environment, that assumption may no longer hold.

To support this shift, industry participants could begin rethinking how agents interact with the broader payments ecosystem – securely, transparently and at scale. At Visa, we aim to help shape a trusted AI commerce environment through initiatives like Visa Intelligent Commerce – by developing new payment capabilities, supporting standards development and collaborating with leaders across the AI ecosystem.



About Visa Consulting & Analytics

Visa Consulting & Analytics (VCA) helps institutions explore how AI may autonomously make payments on behalf of users, and how financial servi es can evolve to enable, secure, and support this future.

How Visa can support your AI-native payments journey:

Learn	Strategize	Pilot	Expand
Gen AI Immersion Bootcamp	Gen AI Strategy	Gen AI Proof of Concept	Gen AI Infrastructure

Learn: Develop foundational understanding of how AI can transform payment behavior, from user-initiated to AI-initiated.

- Immersion bootcamps on AI.
- Landscape reviews of emerging use cases and technologies.
- Deep dives into agent architectures and payment models.

Strategize: Define our long-term role in an ecosystem where AI systems perform payments independently.

- Design of future-aligned payment strategies and integration paths.
- Exploration of new AI-centric products and value propositions.
- Assessment of regulatory/compliance considerations, landscape and customer needs.

Pilot: Experiment with early-stage use cases that enable or support AI-driven payments.

- Use case identifi ation, prioritization and opportunity sizing.
- Pilot new Visa products (i.e. Visa Intelligent Commerce).
- Proofs of concept for embedded payments in AI platforms.

Expand: Expand from leveraging AI to enabling it, serving as trusted infrastructure for AI agents and autonomous commerce.

- Create partnership to co-create intelligent commerce environments.
- Adjust models and capabilities as the AI landscape matures.

Why Visa Consulting & Analytics: VCA combines deep payments knowledge with expertise in emerging technologies to help clients imagine what's next. We've already helped financial institutions

Design long-term strategies that align with generative AI and autonomous financial beh viors	Explore AI and develop use cases	Prioritize use cases and create an implementation roadmap

Glossary

AI Agent:

a software entity that performs tasks autonomously or semi-autonomously using artificial intelligen e models to make decisions following reasoning frameworks and leveraging tools to go beyond their training data (e.g. access up-to-date information from a website in real time). These agents will be able to initiate, manage, and execute payment transactions, reaching minimal human intervention.

AI app:

a software application that uses artificial intelligen e to perform specific tasks that usually require human intelligence. These tasks can include understanding natural language, recognizing images, making recommendations, and predicting outcomes. AI apps are often consumer-facing, meaning they are designed for direct interaction with users. Examples include virtual assistants like Siri or Alexa, chatbots for customer support and conversational models like Chat GPT.

AI platform:

comprehensive suite of tools, services, and infrastructure that enables developers and businesses to build, deploy, and manage AI applications. These platforms often include services for data storage and processing, machine learning model development and training, API management, and deployment environments. In the realm of AI-first payments, an AI platform might provide the foundational technology for developing and running AI-powered payment agents and related AI apps. Examples include Google Cloud AI Platform or Amazon Web Services AI.

Agent economy:

emerging ecosystem surrounding AI agents, encompassing their creation, deployment, interaction, and the economic value they generate. This includes the development of agent platforms, marketplaces for agents and their capabilities, and the impact of agents on various industries, including payments.

API (Application Programming Interface):

set of rules and specifi ations that enable different software programs to communicate and exchange information. It acts like a digital messenger, defining h w one piece of software can request services from another and how the requested information or action will be delivered back.

API Call:

request made by a client to a server through an Application Programming Interface (API). This request allows the client to access specific functions or data p ovided by the server. They are fundamental in integrating various applications and services, ensuring seamless interoperability within complex software ecosystems.

B2B virtual card tokens:

secure, 16-digit digital token payment method for business-to-business transactions. Linked to a traditional card (PAN), these single- or multi-use tokens enhance security and control for specific payments bet een companies.

Chain-of-Thought:

prompting technique for large language models that encourages them to explicitly generate a sequence of intermediate reasoning steps before arriving at a final an wer.

Data Stores:

they enable language models to access up-to-date and dynamic information, overcoming the limitations of their static training data. Developers can add data like PDFs or spreadsheets directly into the agent's workfl w without retraining the model. This data is often converted into vector embeddings, which the agent can then use to enhance its responses or actions. This is particularly relevant for Retrieval Augmented Generation (RAG) applications, where agents can search and retrieve real-time content from sources like websites or structured documents to inform their actions.

Extension:

they act as a standardized bridge between agents and external APIs, enabling agents to seamlessly execute API calls without needing custom code. For example, an agent could use a "Google Flights API" extension to retrieve fli ht data. Extensions are configu ed as part of the agent and are applied dynamically during runtime, making them efficient an adaptable for various tasks.

Functions:

reusable modules of code that perform specific tasks based on p ogramming logic. Unlike Extensions, Functions are executed on the client-side (outside the agent's core architecture). They are useful when API calls or specific ope ations need to occur outside the agent's main process, often due to security constraints or architectural choices. This decoupling allows developers more flexibility and ontrol over certain operations.

GPT (Generative Pre-trained Transformer):

refers to a family of large language models, developed by OpenAI, that leverage deep learning techniques to generate human-like text. These models are pre-trained on vast amounts of text data, allowing them to understand and produce coherent and contextually relevant language. They serve as a foundational technology for AI applications that require advanced language understanding and generation.

Hyperscalers:

companies that provide massive, scalable cloud computing services, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). They often provide the underlying infrastructure and services that power AI payment systems and the agents that operate within them.

Large Language Model (LLM):

type of artificial intelligen e model, typically based on deep learning, that has been trained on a massive amount of text data. These models excel at understanding and generating human-like language, making them a core component in many AI agents used for tasks such as understanding payment instructions, generating payment confirmations, or providing customer support.

Multi-agent workfl ws:

scenarios where multiple AI agents interact and collaborate to achieve a common objective, particularly in the context of payment processes. For example, one agent might handle user authentication, another might process the payment transaction, and a third could manage post-payment notifi ations and reconciliation, creating a coordinated and efficient payment w.

Multi-level permissioning:

security mechanism that allows for granular control over access and actions within a payment system. Different levels of permissions can be assigned to various entities (e.g., users, agents, roles), ensuring that only authorized agents can perform specific payment operations, enhancing security and compliance.

Open banking:

regulatory framework that allows third-party financial servi e providers to access a consumer's banking information (with their explicit consent) through secure APIs. This enables the development of innovative financial p oducts and services, potentially allowing AI models to initiate payments, retrieve account details, and manage finan es on behalf of users in a secure and regulated manner.

Online travel agencies (OTAs):

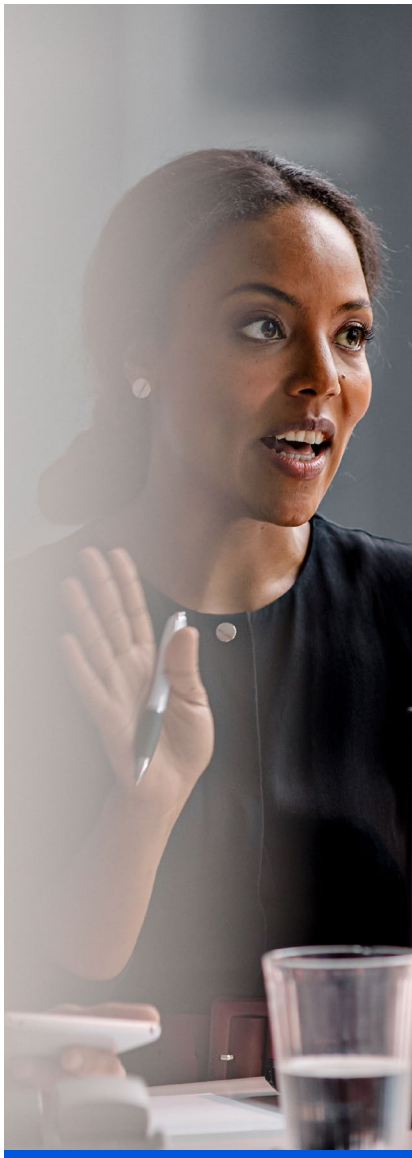
web-based platforms that allow users to book travel-related services such as fli hts, hotels, and car rentals. Examples include Expedia, Booking.com, and TripAdvisor. For these platforms, retail users pay the OTAs, which in turn tend to pay their providers in a second transaction with B2B virtual card token.

Pass-through digital wallet:

transactions initiated using pass-through digital wallets transmit the customer's payment credential (usually tokenized) to the merchant, who then processes the transaction directly with their acquirer like any other Visa payment transaction.

Payment orchestration:

process of managing and streamlining the fl w of payment transactions across multiple payment methods, providers, and channels. It involves intelligently routing payments, handling failures, and ensuring a seamless and efficient payment experie e.



Payment Passkey:

private, biometric-based authentication credential linked to a device-bound cloud token, which is securely stored on a cardholder's trusted device after successful identity verifi ation. Once created, it utilizes the local platform authenticator (such as biometrics) on the device to ensure that only the cardholder who completed identity verifi ation can access the token. By combining inherence factors (biometrics) with possession factors (the trusted device), a payment passkey enables issuers to confirm cardholder identity with a high degree of confiden e.

Plugin:

software component that adds specific eatures or functionalities to a larger, existing software application or system. Plugins enable customization and extend the capabilities of the host application without altering its core structure.

Proto agents:

early-stage or foundational versions of AI agents, often with a limited set of capabilities, used for experimentation, prototyping, or as building blocks for more complex and sophisticated payment agents.

ReAct (Reason + Act):

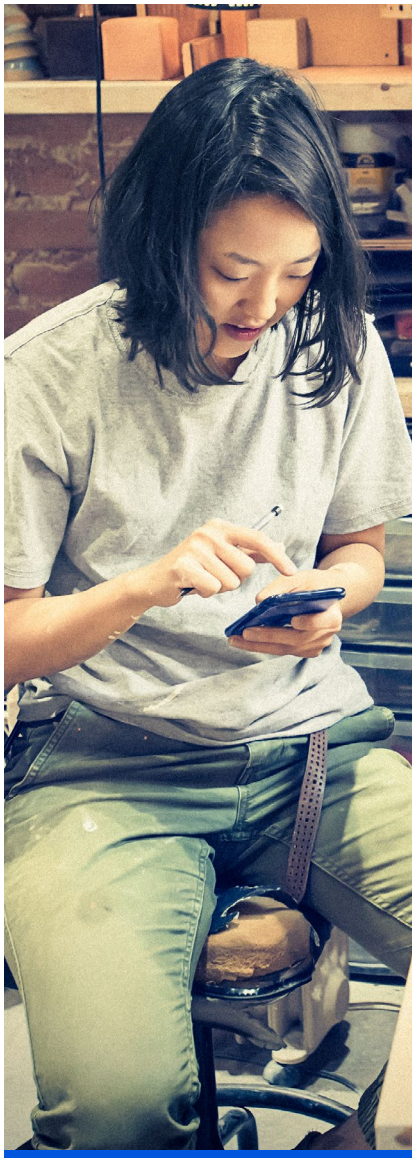
prompting technique used with large language models that integrates a thought process strategy for models to interleave reasoning steps ("Thought") with taking actions ("Action") to solve tasks. This approach helps AI agents to break down complex payment-related tasks into manageable steps, improving their ability to make informed decisions and execute them effectively.

Research preview:

early release or demonstration of a technology or product, often with limited functionality or support, intended for research purposes and to gather feedback from the research community.

Retrieval Augmented Generation (RAG):

AI framework that enhances the knowledge of a language model by allowing it to retrieve information from external data sources (like documents, databases, or the web) and use that information to generate more accurate and contextually relevant responses or actions. This is particularly useful for AI agents in payment scenarios where access to up-to-date information or specific data is equired for tasks like fraud detection or personalized offers.



SCA (Strong Customer Authentication):

regulatory requirement, primarily within Europe, for verifying electronic payments. It mandates the use of at least two out of three authentication factors: something the customer knows (e.g., password or PIN), something the customer possesses (e.g., a mobile phone or hardware token), and something the customer is (e.g., fingerprint or facial recognition). This is a critical security measure for AI payments, ensuring that transactions initiated or managed by AI models are securely authenticated.

SDK (Software Development Kit):

collection of software development tools, libraries, documentation, code samples, and processes that allow developers to create applications for a specific plat orm, framework, or system.

Staged digital wallet:

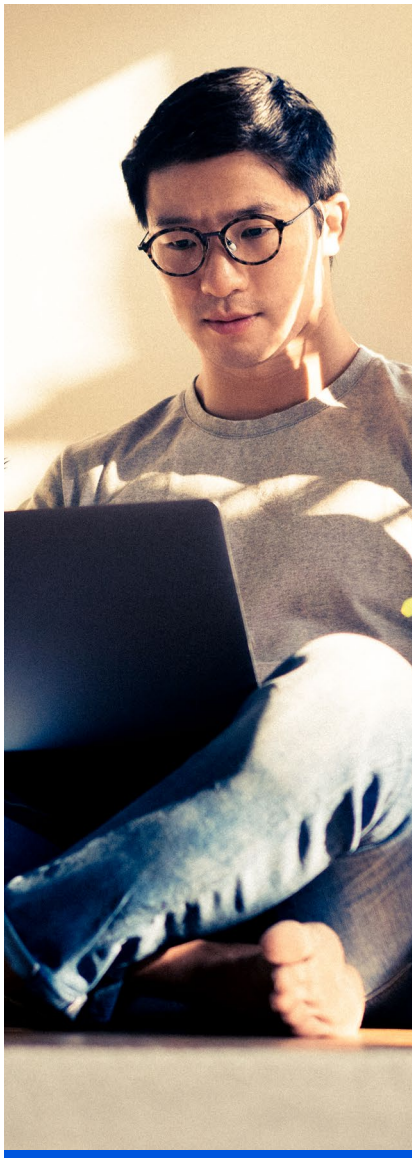
staged digital wallets assign a separate "account" to the customer, which the customer may pre-load with funds, but may also facilitate "back-to-back funding" transactions, permitting the customer to undertake transactions with sellers or other users on the digital wallet's platform when there are not sufficient funds in the digita wallet-assigned account to complete the transaction.

Token:

in the context of payments and security, a token is a surrogate value, typically a string of characters, that replaces sensitive data such as credit card numbers or bank account details. This process, called tokenization, enhances security by ensuring that the actual payment information is not stored, processed, or transmitted in plain text by AI agents or other systems involved in the payment process.

Tree-of-Thought:

extension of the Chain-of-Thought technique that allows an AI agent to explore multiple reasoning paths in a tree-like structure. This enables an AI agent to consider different options, backtrack if necessary, and ultimately choose the most appropriate course of action for a given payment scenario.



Acknowledgements

Authors of this paper include Alicia Ngomo, Ángel Salinas, Marta Lorca and Carmen Lázaro.

The authors would like to thank Claudio Di Nella and the Global Product Team for their input and review.

Sources

All brand names, logos and/or trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.

All below references, links and sources accessed: June 2025.

1. Visa (2025), Visa Product Drop event. Visa: Visa Product Drop Event
2. *US Consumer Agentic Ecommerce Survey* (concept test February 2025) commissioned by Visa (survey of 998 online shoppers who own a debit or credit card)
3. OpenAI (2025), Improved shopping results from ChatGPT search. OpenAI: Improved Shopping Results from ChatGPT Search
4. Marlow, P., Wiesinger, J., & Vuskovic, V. (2024). *Agents*. *Github:* Google AI Agents Whitepaper
5. Anthropic (2024). Building effective agents. Anthropic: Anthropic Building Effective Agents
6. Anthropic (2024). Introducing the Model Context Protocol (MCP). Anthropic: Anthropic Introducing the Model Context Protocol
7. Bereczki, T., & Liber, Á. (2024). The state of web scraping in the EU. IAPP: IAPP The State of Web Scraping in the EU
8. Perplexity (2024). Shop like a pro: Perplexity's new AI-powered shopping assistant. Perplexity: Perplexity Shop Like a Pro
9. Stripe (2024). Adding payments to your LLM agentic workflows. Stripe: Strip Adding Payments to your LLM Agentic Workflows
10. Fintech Brainfood (2025). Rant: Wallet wars pt 3 – Authentication for AI Agents. Fintech Brainfood: Fintech Brainfood Rant: Wallet Wars Pt 3

Disclaimers

This document is intended for illustrative purposes only. It contains depictions of a product, service or solution (the "Product") currently in the process of development or deployment and should be understood as only a representation of the potential features of a fully deployed Product. Visa is under no obligation to make this Product available, and versions of this Product, if any, may not contain the features described in this document.

This document contains forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995 that relate to, among other things, our future operations, developments, strategies, and business growth. Forward-looking statements generally are identified by words such as "believes," "estimates," "expects," "intends," "may," "projects," "could," "should," "will," "continue" and other similar expressions. All statements other than statements of historical fact could be forward-looking statements, which speak only as of the date they are made, are not guarantees of future performance and are subject to certain risks, uncertainties and other factors, many of which are beyond our control and are difficult to predict. We describe risks and uncertainties that could cause actual results to differ materially from those expressed in, or implied by, any of these forward-looking statements in our filings with the SEC. Except as required by law, we DO NOT intend to update or revise any forward-looking statements as a result of new information, future events or otherwise.

The projections and growth estimates contained in this document are based on historical data, current market trends, and a variety of assumptions. These projections are intended for informational purposes only and should not be interpreted as guarantees of future performance. While we strive to provide accurate and realistic forecasts, numerous factors, including but not limited to market volatility, economic changes, and unforeseen circumstances, can influence actual outcomes. Consequently, there is no assurance that the clients will achieve the projected growth levels. We recommend that clients consider these projections as one of many tools in their decision-making process and consult with Visa Consulting and Analytics for personalised advice.

Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or "best practices" may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. All brand names, logos and/or trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.