QuantumBlack
AI by McKinsey

The agentic commerce opportunity: How AI agents are ushering in a new era for consumers and merchants

October 2025

Agentic AI promises to radically remake the entire shopping experience. Here's a glimpse into the near future—and what merchants, players, and platforms need to know in order to thrive.

by Katharina Schumacher and Roger Roberts
with Katharina Giebel

Contents

At a glance

- **Agentic commerce—**shopping powered by AI agents acting on our behalf—represents a seismic shift in the marketplace. It moves us toward a world in which AI anticipates consumer needs, navigates shopping options, negotiates deals, and executes transactions, all in alignment with human intent yet acting independently via multistep chains of actions enabled by reasoning models.
- This isn't just an evolution of e-commerce. It's a rethinking of shopping itself in which the boundaries between platforms, services, and experiences give way to an integrated intent-driven flow, through highly personalized consumer journeys that deliver a fast, frictionless outcome.
- The stakes are high: By 2030, the US B2C retail market alone could see up to $1 trillion in orchestrated revenue from agentic commerce, with global projections reaching as high as $3 trillion to $5 trillion, according to McKinsey research.
- This trend will have the breadth of impact of prior web and mobile-commerce revolutions, but it can move even faster since agents can traverse the same digital paths to purchase as humans, allowing them to "ride on the rails" laid down by these prior revolutions.
- This presents both benefits and risks for today's commerce ecosystem. All kinds of businesses—brands, retailers, marketplaces, logistics and commerce services providers, and payments players—will need to adapt to the new paradigm and successfully navigate the challenges of trust, risk, and innovation.
- From a technical standpoint, that means mastering and deploying emerging integration enablers like Anthropic's Model Context Protocol (MCP), Agent-to-Agent (A2A) Protocol, Agent Payments Protocol (AP2), and Agentic Commerce Protocol (ACP) that enable a new era of intelligent, autonomous agents. It also means fundamentally re-architecting approaches to identity management and loyalty. Smart organizations are already beginning to create new, agent-ready sites that provide both strong agentic and consumer experiences.
- Business models will also have to change to thrive in an agent-driven economy. This means exploring new monetization strategies and new marketing and customer engagement approaches. For many intermediaries in today's shopping flow, a key choice will be whether to launch your own agents and when and how to welcome agentic traffic. These could be existential choices for some businesses.
- Agentic commerce requires a fundamental rethinking of how value is created, captured, and delivered. Companies that adapt quickly will not only meet evolving consumer expectations but also redefine their industries. Those that hesitate risk losing ground as AI agents become the new gatekeepers of commerce.

CHAPTER 1

A new kind of shopping experience—seamless, efficient, and mediated by AI agents

Imagine that a promising new job opportunity requires you to relocate your family across the country. Chances are that whatever excitement you feel about the new role is soon tempered by the innumerable hassles of moving. You need to find a comfortable home with a manageable commute, decide what to bring and what to sell, and engage a trustworthy moving company to deliver everything on time. Then there's the issue of finding new doctors, veterinarians for the pets, a gym, and after-school programs for the kids. It's overwhelming.

Now imagine that you had an autonomous AI agent to handle these tasks for you. With a deep understanding of your budget, lifestyle, commute preferences, kids' hobbies, and even your pets' needs, the agent can get to work. To research neighborhoods and housing options, it synthesizes data from multiple sites and platforms, scanning myriad real estate listings and recommending the most appealing choices. When you e-sign your lease, the agent reviews the terms to ensure anything atypical is highlighted and gets your attention.

You have a place; now, on to your stuff. Is it worth $700 to ship this dresser, or should you sell it for $200 and buy a new one when you arrive? If the latter, what are the options? You snap photos of your furniture, and the agent assesses resale value, lists items for sale on various platforms, and negotiates sales on your behalf. For new items, it sources local options that fit your style and budget, simulating what fits in your new apartment and offering interior design suggestions, and then makes the purchases once you've approved them. As for the move itself, the agent manages it all, coordinating with movers, scouring local retailers for the things you'll need for your new home, and syncing deliveries so that everything arrives when it should.

In the traditional world of commerce, accomplishing this would require navigating a dozen different tools, websites, online marketplaces, and retail stores. In the agentic era, the AI agent does much of this for you, serving as your personal strategist, designer, negotiator, and logistics manager. It makes microdecisions across multiple dimensions—budget, aesthetics, logistics—transforming a stressful, fragmented journey into something personalized, highly efficient, and coherent.

From chaos to coordination: This is agentic commerce

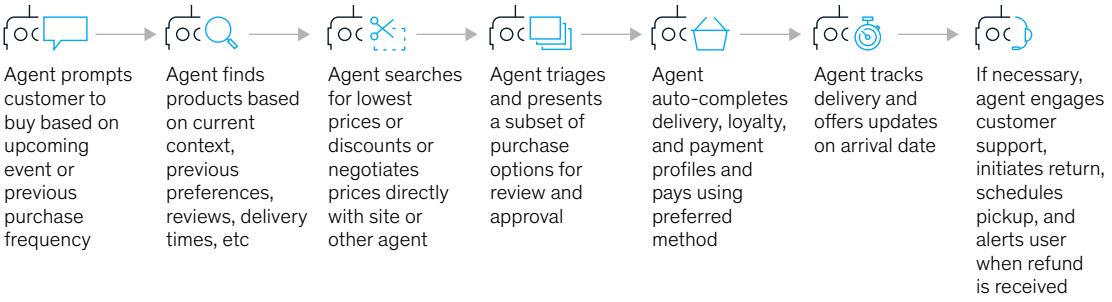
What is agentic commerce? In the simplest terms, it is shopping powered by intelligent AI agents capable of anticipating, personalizing, and automating every step of the process to create frictionless, proactive experiences (Exhibit 1). Enabled by cutting-edge advancements in AI, agentic commerce represents a transformative shift in the digital marketplace. It will not just enhance the way we buy and sell—it's a potential paradigm shift that could redefine the entire commercial ecosystem. Consumer behavior is already beginning to change: 44 percent of users who have tried AI-powered search say that it has become their "primary and preferred" source for internet searching, compared with 31 percent who prefer using traditional search, according to recent McKinsey research.[1]

[1] McKinsey AI Discovery Survey; see also "A new front door to the internet: Winning in the age of AI search," forthcoming on McKinsey.com.

Exhibit 1

AI agents promise to transform the consumer experience.

Potential agentic customer journey



McKinsey & Company

As commerce evolves beyond the human-readable web, agents stand to become a primary interface between users and marketers, fundamentally transforming how consumers interact with products and services. It's a transformation akin to the e-commerce revolution—only it's likely to happen quite a bit faster. Consider that in 1999, 100 million internet users[2] (just under 2 percent of the global population[3]) began exploring e-commerce. In 2025, nearly 5.6 billion users[4] are connected to the internet, representing approximately 68 percent of the world's population.[5] In this hyperconnected age, dramatic shifts at a much larger scale can occur much more rapidly. In the early days of e-commerce, many who lagged found themselves left behind or even out of business. Now, as then, companies need to figure out how to adapt to this emerging new reality—even if it means rethinking their existing business models—or risk a similar fate.

> "Companies have spent decades refining consumer journeys, fine-tuning every click, scroll, and tap. But in the era of agentic commerce, the consumer no longer travels alone. Their digital proxies now navigate the commerce ecosystem, making millions of microdecisions daily. To thrive, brands must rethink the full stack of engagement—not for the people they've worked to understand but for the agents now acting on their behalf."
>
> —**Becca Coggins,** McKinsey senior partner and global leader of the Retail and Consumer Packaged Goods Practices

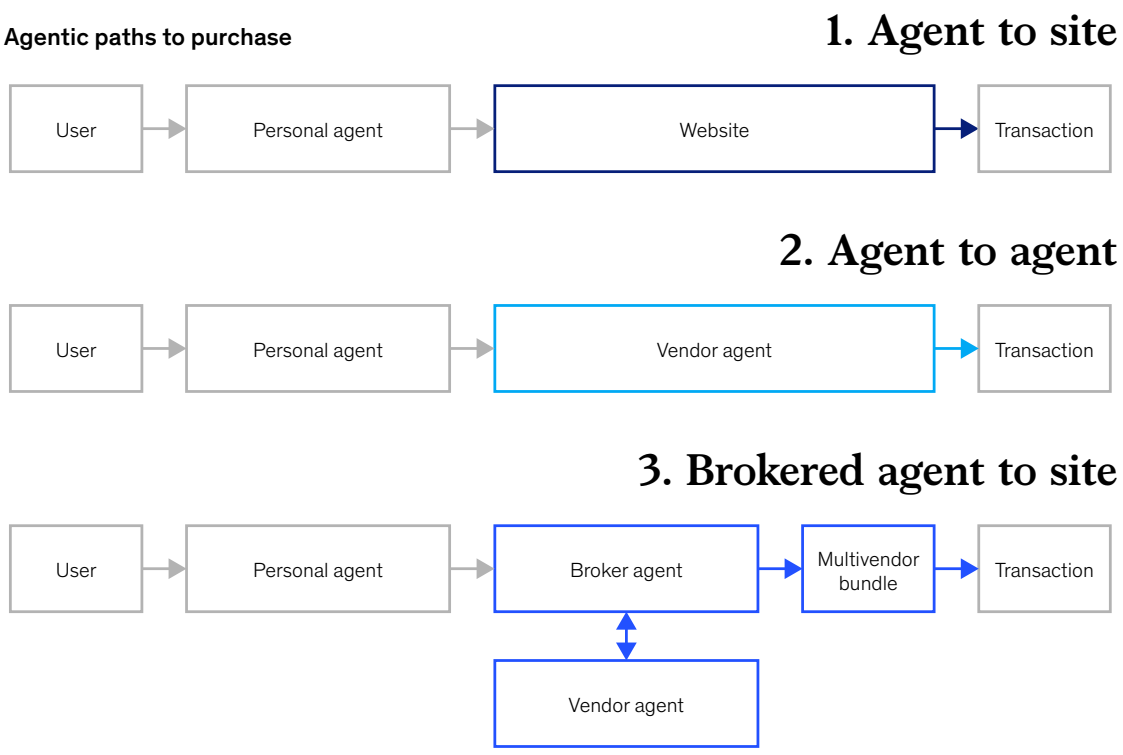
2 "Internet users now exceed 100 million," *New York Times*, November 12, 1999.
3 *The world at six billion*, United Nations, October 12, 1999.
4 "Internet usage worldwide - statistics & facts," Statista, April 11, 2025.
5 "Current world population," Worldometer, accessed October 1, 2025.

Agentic commerce is taking shape through three key interaction models: agent to site, agent to agent, and brokered agent to site (Exhibit 2).

1. *Agent to site:* Agents interact directly with merchant platforms. For example, a travel agent scans multiple hotel websites, highlighting those that fit your preferences and confirming your interest before booking the room.
2. *Agent to agent:* Agents transact autonomously with other agents. For example, a personal-shopping agent communicates with the in-house AI commerce agent of a retailer to, say, negotiate a bundle discount across items in different departments.
3. *Brokered agent to site:* Intermediary systems facilitate multiagent and multiplatform interactions. For example, a restaurant-booking agent contacts the broker agent of a platform like OpenTable, which finds you a table and applies loyalty discounts based on your profile.

Exhibit 2

Three possible paths to purchase in an agentic world.



McKinsey & Company

As these models evolve, the way commerce is structured will shift, with manual search and comparison gradually being replaced by a machine-mediated process, with agents increasingly augmenting human decision-making. While the pace and extent of agentic AI is still unclear, the technology is improving rapidly, and integration is less difficult and expensive than prior platform transitions, so even a scenario with moderate assumptions indicates immense economic value. Considering the growing availability and adoption of AI-powered discovery tools, along with moderate assumptions about merchant readiness for agentic commerce, by 2030, the US B2C retail market alone could represent an opportunity to orchestrate revenue in the range of $900 billion to $1 trillion. Globally, this opportunity is projected to range from $3 trillion to $5 trillion, McKinsey research has found.[6] (These figures only reflect goods and do not yet include services; nor do they account for the significant B2B marketplace.)

The agentic era will see a shift from traditional vertical destinations toward a more integrated, horizontal-agent ecosystem that supports cross-functional and cross-intent consumer behavior. This means that the conventional idea of visiting a specific platform to accomplish a task—say, using Amazon for shopping or Expedia for booking travel—will give way to new modes of commerce. Rather than navigating between platforms based on specific objectives, personal agents, functioning like concierges, will be able to take care of all consumer needs when their intent is first voiced or surfaced. In the corporate world, agents will be embedded in applications—allowing employees, for example, to book business travel within everyday tools, such as Slack, without having to leave the app. This unbundles and "de-verticalizes" shopping for services and goods, forcing companies to rethink and innovate beyond the status quo.

The broad outline of this world is already taking shape. Half of all consumers now use AI when searching the internet.[7] And what begins as AI-mediated discovery increasingly carries through to execution, as AI agents compare options, assemble baskets, and complete checkout via emerging payment protocols and merchant integrations. The AI platform Perplexity, for example, launched an agentic shopping tool, "Perplexity Buy with Pro," in late 2024. OpenAI's Operator, launched in January 2025 and now integrated into ChatGPT, uses agents to help users automate tasks like booking travel and restaurant reservations. More recently, OpenAI announced an Agentic Commerce Protocol, codeveloped with Stripe, which allows users to complete purchases within ChatGPT without leaving the chat. Shopify is developing an agentic shopping infrastructure that allows agents to tap into its catalog and build carts across merchants. Amazon, Google, PayPal, Mastercard, and others are also developing agentic shopping services. Collectively, these moves are turning agentic commerce from a concept to an imminent reality.

For retailers, this is the time to ask bold questions, including:

— What opportunities will agentic commerce create, and which ones will it diminish?

— How can you build strong bonds with consumers as your shoppers shift to commerce mediated by agents? How can you ensure your systems act on behalf of your customers?

— How can your business become indispensable in an agent-driven economy? What new revenue models can you pioneer in a world where agents are the gatekeepers of consumer intent?

This report will help leaders better understand how to address these questions. The hypothetical cross-country move described above illustrates what the agentic era means for consumers. Next, we'll address the implications for business models, technology infrastructure, and the business–consumer relationship itself.

[6] McKinsey market research early estimations are based on US Census data and forecasted adoption rates.
[7] McKinsey AI Discovery Survey; see also "A new front door to the internet: Winning in the age of AI search," forthcoming on McKinsey.com.

CHAPTER 2

Creating the infrastructure for agentic commerce

As we move toward this new era in digital commerce, agentic commerce is being sculpted by the hands of developers, who are creating and refining systems that seamlessly integrate APIs from multiple sources to deliver real-time information and dynamic customer experiences. The pace of technological advancement is staggering. The duration of tasks that large language models (LLMs) can reliably complete with at least a 50 percent success rate has been doubling every seven months since 2019, according to METR.[8] In 2019, for example, leading models could only manage tasks requiring a few seconds of human effort. In 2025, Anthropic's Claude 3.7 Sonnet boasts a "time horizon" of 59 minutes, capable of completing tasks that would take a skilled human nearly an hour—and recently, Claude 4.5 has extended this to more than 30 human hours. This marks an inflection point where AI may soon be able to tackle multiday or multiweek tasks, opening up new opportunities in task specialization and multiagent collaboration.

The rapid pace of innovation in agentic AI is being driven by six key tools and developments:

— *Model Context Protocol.* MCP is an interoperability standard that allows AI agents and systems to share context, intent, and data about prior activities across models and tools. Unlike static prompts or isolated API calls, MCP enables persistent, structured communication, allowing agents to retain memory, reasoning, and objectives across environments. By standardizing how developers connect LLM-based applications to tools and function calls, MCP empowers agents to take meaningful actions across platforms, unlocking more coherent, autonomous, and context-aware behavior and laying the foundation for truly agentic ecosystems (Exhibit 3).

— *Agent-to-Agent Protocol.* A2A is a communication protocol and interaction model that empowers autonomous AI agents to coordinate, negotiate, and complete tasks directly with one another, minimizing the need for human intervention. Built for interoperability, A2A enables agents—regardless of vendor, architecture, or environment—to securely exchange capabilities, status, and context through standardized protocols like JSON-RPC and HTTP. This open framework supports long-running tasks, dynamic capability discovery, and multimodal collaboration, including text, audio, and visual outputs. By reducing integration overhead and facilitating cross-agent coordination, A2A establishes the foundation for scalable, multiagent ecosystems. This accelerates enterprise adoption of autonomous workflows and allows intelligent agents to operate efficiently in real-time, cross-platform marketplaces.

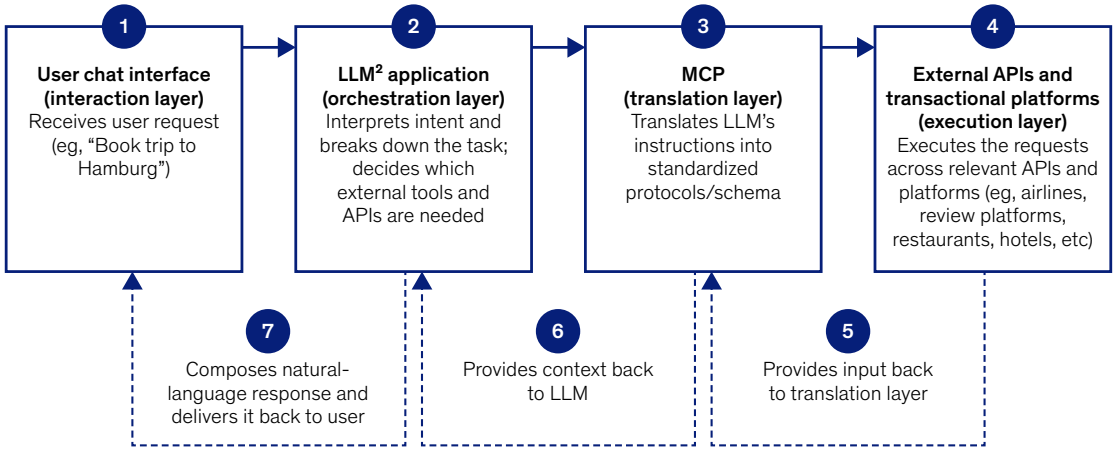
— *Agent Payments Protocol.* Google's AP2 is a groundbreaking open, payment-agnostic protocol designed to empower autonomous and semiautonomous AI agents to make verifiable purchases on behalf of users. By utilizing cryptographically signed mandates that link intent, cart, and payment across users, merchants, and payment networks, AP2 creates an audit trail, not subject to repudiation, ensuring transparency and accountability. This innovative protocol has the potential to revolutionize the way transactions are conducted by unlocking new revenue streams through automated execution of "standing intents," reducing costs by minimizing fraud and chargebacks, and reshaping competition as agent routing algorithms optimize for cost, speed, and rewards.

[8] "Measuring AI ability to complete long tasks," METR, March 19, 2025.

Exhibit 3

The Model Context Protocol standardizes how large language models connect to tools and take action across platforms.

How the Model Context Protocol (MCP)[1] translates consumer intent into a successful agentic transaction



[1]An interoperability standard that enables AI agents and systems to share context, intent, and state across models and tools through a standardized protocol. This protocol underpins more coherent, context-aware, and collaborative agentic behavior, forming the connective tissue between models, tools, and tasks in AI ecosystems.
[2]Large language model.

McKinsey & Company

— *Computer use agent.* This system allows AI to control user interfaces, such as a mouse and keyboard, to complete tasks like executing purchases or filling out online forms. Developers are creating tools and frameworks that enable AI to interact with websites and user interfaces, automating tasks without direct human input. These systems are particularly useful when APIs are unavailable or impractical, especially for niche cases where building an API isn't cost-effective.

— *Contextual AI-driven personalization.* This capability marks a shift from static, search-based predictions to dynamic, context-aware AI that adapts to changing user intent. By memorizing user preferences and inferring details from interactions, these agentic systems provide relevant and personalized recommendations. Developers are building context-aware AI systems that dynamically adapt to user intent, implementing memory-driven architectures that capture and infer user preferences, ensuring real-time personalization that responds to evolving contexts.

— *Dynamic planning with real-time adjustment.* This refers to the ability of agentic systems to offer an end-to-end dynamic customer experience with real-time updates and adjustments—for example, executing a complex travel itinerary that includes flights, hotels, restaurants, and ticketed events, with automated expense integration and tracking. Developers are creating systems that integrate APIs from multiple partners to offer real-time updates, alternative products/services, and automated adjustments to plans, expenses, and reporting, ensuring outcomes are machine readable.

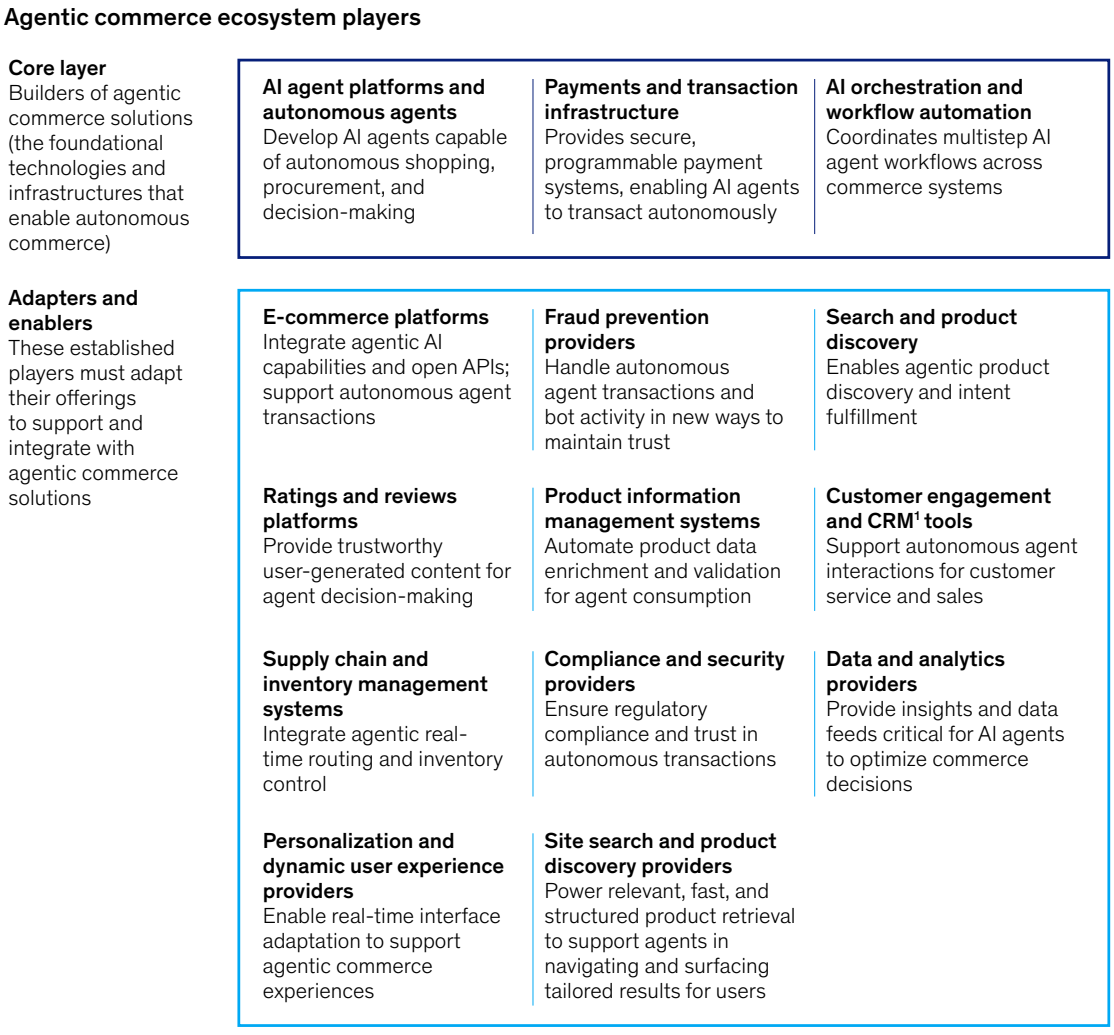
As developers continue to innovate, the landscape of agentic commerce will evolve, offering opportunities for businesses and consumers alike.

What does the agentic ecosystem look like?

Just as traditional online commerce relies on a wide ecosystem of players—e-commerce platforms, search engines, payment providers, review sites, logistics, and fraud prevention tools—agentic commerce will require a similarly diverse and interconnected system (Exhibit 4). At its core, the agentic ecosystem includes AI platforms, autonomous agents, infrastructure, payment systems, and workflow automation. But equally important are the adapters and enablers—such as traditional e-commerce platforms and fraud prevention solutions—that must evolve to support this new paradigm. The adoption and scaling of agentic commerce will depend on the speed with which these players make their systems agent compatible and widely adoptable by consumers, retailers, and brands.

Exhibit 4

Within the emerging agentic commerce ecosystem, adapters and enablers will determine the pace at which core players redefine commerce.



[1]Customer relationship management.

McKinsey & Company

As commerce transitions from direct user interactions to agent-initiated transactions, the existing payments infrastructure will encounter significant structural challenges. Traditionally, components such as gateways and fraud engines have been built around a human-in-the-loop model, in which identity, intent, and authorization are explicit and observable. Agentic commerce disrupts this paradigm: The "customer" is now an AI agent acting on behalf of a person, which necessitates new approaches for delegated authorization, programmable spend policies, and consent attestation. This shift demands that the current risk stack evolve from relying on behavioral heuristics to establishing protocol-level trust—verifying not just users but the agents themselves.

Simultaneously, a burgeoning array of risk, compliance, and identity providers must adapt existing know-your-customer and anti-money-laundering (KYC/AML) standards to accommodate agent identification—know your agent (KYA)—and develop new fraud detection models able to address agent behavior, compromised agent credentials, and potential multiagent attacks. Additionally, tokenization, dispute resolution, and real-time settlement systems may require enhancements to support A2A Protocols and incorporate richer context within transaction metadata. As the landscape of commerce continues to evolve, these adaptations will be crucial in ensuring a secure and efficient payments ecosystem.

Both emerging and legacy players are investing in innovative solutions for merchants and customers. In September 2025, Google launched AP2,[9] a significant change for agent-led transactions. This secure, open standard is backed by industry leaders such as Mastercard, PayPal, American Express, Adobe, and Alibaba. It ensures trust through cryptographically signed mandates, which provide verifiable and auditable processes, a cornerstone for building trust in agentic commerce.

Meanwhile, payment industry leaders are pursuing parallel innovations. Mastercard is developing its Agent Pay solution, and industry groups are working to extend Worldwide Web Consortium (W3C) verifiable credentials into payments. At the same time, Visa is positioning its global network as the backbone of agentic commerce. In partnership with AI platforms such as Anthropic, IBM, Microsoft, Mistral AI, OpenAI, Perplexity, Samsung, and Stripe, Visa is piloting transactions where AI agents can spend on behalf of users within preset budgets and consent parameters.[10] Visa has also launched AI-ready cards, which replace static-card details with tokenized digital credentials—enabling merchants to verify that a consumer's agent is truly authorized to act on their behalf.

The catalyst for this new form of commerce is found not only in established players but also in breakthrough innovation from start-ups in Silicon Valley and beyond. One example is Skyfire, which recently launched Agent Checkout, powered by a protocol dubbed KYAPay—an open standard that equips AI agents with verified identities and programmable payment capabilities, facilitating identity verification, auditability, spend control, and reputation tracking. Compatible with existing authentication systems, APIs, and MCP servers, Skyfire has onboarded partners like APIFY, BuildShip, CarbonArc, and Forter,[11] supporting seamless monetization and agent interaction through standardized tools.

These developments highlight two key trends in the payments landscape: the emergence of new innovations designed to meet the unique demands of agentic transactions, ensuring security and efficiency; and moves by established networks and platforms to equip legacy systems with features like programmability and delegated authorization to provide trusted rails for autonomous transactions. As agentic commerce evolves, these complementary streams—innovation at the infrastructure level and reinvention from within—are both crucial for unlocking safe, seamless, agent-enabled payments. Together, they pave the way for a future where AI agents can transact autonomously, securely, and efficiently.

[9] "Powering AI commerce with the new Agent Payments Protocol (AP2)," Google Cloud, September 16, 2025.
[10] "Find and buy with AI: Visa unveils new era of commerce," Visa press release, April 30, 2025.
[11] "Skyfire launches Open KYAPay Protocol with Agent Checkout," Business Wire, June 26, 2025.

> "Agentic commerce will push payments providers to evolve in many ways. Authentication and fraud prevention will become more complex, moving from stopping bots from making transactions to enabling the right agents to transact for customers. Agentic commerce is also likely to shift some of the control of subscription models and card-on-file payments from merchants to consumer agents. And consumer payments players will have to rethink how they acquire new customers while retaining top-of-wallet status among consumers who are increasingly evaluating products through an agent."
>
> —**Marie Claude Nadeau,** senior partner and global leader of McKinsey's payments work

As new API strategies and platform interfaces emerge, businesses should stay agile and ready to adapt to new approaches and integrations. The focus should be on developing robust, optimized APIs that facilitate seamless agent interactions, such as between automated agents and virtual assistants. In doing so, businesses should consider three strategic implications:

- *Lead in AI development.* Build a strong technological foundation to position your business at the forefront of AI innovation. Future-proof your core brands by integrating advanced AI capabilities as technology evolves.
- *Adopt a modular strategy.* Avoid relying solely on exclusive partnerships with leading AI platforms. Instead, embrace a modular, flexible strategy grounded in a robust API infrastructure. This approach ensures your business remains adaptable and in control, even as the AI landscape shifts with new entrants like DeepSeek or Manus AI, which could drive competition and alter market dynamics.
- *Forge strong connections with Silicon Valley and other innovation hubs.* Establish a close-knit network with developers, start-ups, and incubator programs in the epicenter of AI innovation. Consider basing teams there to stay at the cutting edge of AI advancements and maintain a competitive edge in the evolving digital landscape.

CHAPTER 3

Business model evolution in the era of agentic commerce

In 1942, the economist Joseph Schumpeter coined the term "creative destruction" to describe the power of innovation and new technologies to destroy existing economic structures—jobs, companies, even entire industries—while simultaneously laying the groundwork for new structures to emerge. The emergence of agentic commerce represents precisely this kind of moment for business leaders.

Adapting to this paradigm shift will require more than a user interface refresh. Instead, it means grappling with a fundamental restructuring of how products are discovered, how buying decisions are made, and how customer relationships are formed and maintained. After all, in an agentic world, your customer may no longer be a human with a browser—it is just as likely to be an autonomous agent, acting on that customer's behalf.

We are currently in a phase of rapid experimentation—the future shape of the customer journey remains uncertain. It is safe to say, however, that the widespread adoption of AI-enabled conversational interfaces—ChatGPT now has more than 800 million weekly users,[12] and Google's AI overviews powered by Gemini now reach more than 1.5 billion users[13] per month—means commerce will increasingly flow through AI channels, impacting billions of consumers and tapping into a significant share of global disposable income. In this hyperconnected age, dramatic shifts can occur rapidly; as agentic-interaction models are tested in the market, consumers will begin to express their preferences through their behavior. As they do, businesses will be forced to rethink how they engage with customers, optimize operations, and deliver value—in many cases, fundamentally reinventing traditional business models. It won't be the first time a new technology has forced these kinds of changes. Historically, each wave of technological disruption has reshaped where value is captured, and the AI/API disruption will be no exception.

How will businesses respond to agentic commerce? At a minimum, product directories will need to be optimized for agent readability. Many companies will pilot new agent-first experiences. And others will reimagine their models entirely, owning the orchestration and becoming indispensable in an AI-agent-driven ecosystem. But one thing is certain: Remaining static is not a viable option.

[12] Rebecca Bellan, "Sam Altman says ChatGPT has hit 800M weekly active users," TechCrunch, October 6, 2025.
[13] "Alphabet announces first quarter 2025 results," Alphabet earnings release, April 24, 2025.

> **"This is not a wait-and-see moment. Before long, nearly all retailers will have to grapple with the fact that a significant percentage of their customers will not be human users but rather AI agents. The challenge will be to get out in front of it now, before your rivals do. The companies that move first, even in small ways, will be the ones that help shape the future."**
>
> —**Lareina Yee,** senior partner, director of technology research at the McKinsey Global Institute, and cohead of global ecosystems and alliances

Innovate or renovate? Six key domains businesses should consider

To thrive in the agentic era, retail businesses will have to address six key domains of their business models: 1) customer engagement and product discovery; 2) "clienteling" and loyalty; 3) core commerce platforms; 4) payments and fraud detection; 5) in-store point of service; and 6) fulfillment and returns. The challenge for businesses will be to think strategically about each of these areas—discerning where to innovate (building entirely new strategies and structures) and where to renovate (upgrading existing systems and processes to perform in an AI-native environment).

In three of these domains, innovation will be paramount. To drive engagement and discovery, companies need to develop agents capable of understanding customer intent and proactively suggesting products, services, bundles, or other alternatives. This will require embedding semantic and behavioral metadata into product catalogs, while also developing agent-authenticated interfaces for autonomous discovery and verifying intent and identity in real time to ensure that transactions are both secure and efficient. Driving clienteling and loyalty, meanwhile, will demand new experiences that are hyperpersonalized, with offers triggered by inferred intent. This will require building persistent customer-context layers that are accessible by agents and exposing loyalty services and eligibility engines via APIs.

Renovation, by contrast, will be essential in areas where legacy systems hinder AI integration. Core commerce platforms, for example, should be revamped to enable agents to execute structured transactions with minimal human input, incorporating AI capabilities like dynamic pricing or inventory-aware recommendations. In-store point-of-service systems must be retooled to synchronize digital and physical journeys by sharing context with store associates, accessing digitized store maps and inventory, and integrating spatial computing for in-store navigation. Finally, fulfillment-and-return systems will need agents able to automate fulfillment decisions, negotiate return logic, and orchestrate postpurchase actions—which will require agent-ready fulfillment orchestration APIs and integration with multicarrier and last-mile brokers through modular connectors.

Collectively, these domains form the backbone of an agent-ready commerce stack, and a merchant's ability to thrive in an AI-native future will likely hinge on its ability to adapt across all six.

In order to prepare for an agentic future, merchants can innovate and renovate across 6 key areas

Customer engagement and product discovery

Agent to site
Identifies user intent and requests tailored product sets from brand or commerce platforms

Agent to agent
Communicates preferences to the brand's agent to refine and retrieve options

Agent to broker agent
Compares products, availability, and terms across multiple retailers and presents top picks

Clienteling and loyalty

Agent to site
Tracks past purchases, preferences, and upcoming events to prompt timely re-engagements with brands

Agent to agent
Negotiates perks, previews, or loyalty upgrades based on behavioral signals and tier eligibility

Agent to broker agent
Aggregates loyalty status across brands and reallocates points or perks to match the shopper's goals

Payments and fraud detection

Agent to site
Authenticates and authorizes payments on behalf of users, integrating with merchant payment flows while enforcing delegated consent and spend limits

Agent to agent
Verifies agent identity and intent through cryptographic attestation or identity tokens; enables real-time fraud scoring and trust via protocol-level aent registries

Agent to broker agent
Manages multiparty settlement and risk mitigation across ecosystems, using policy-based authorization, payment abstraction layers, and federated fraud intelligence

Core commerce platforms

Agent to site
Searches, filters, and transacts autonomously when retail systems provide APIs

Agent to agent
Receives structured requests from customer agents, validates parameters, and executes purchases without manual input

Agent to broker agent
Routes requests across multiple commerce systems, optimizing for availability, delivery time, and cost

In-store point of service

Agent to site
Provides real-time in-store navigation based on goals, promotions, and prior behavior

Agent to agent
Exchanges context (intent, loyalty tier) with store agents to personalize service

Agent to broker agent
Ensures continuity across channels, reserving items, syncing carts, and managing handoffs

Fulfillment and returns

Agent to site
Selects fulfillment options aligned with urgency, sustainability, or bundling preferences

Agent to agent
Requests returns, refunds, exchanges, or resale pathways based on context and policy

Agent to broker agent
Balances speed, cost, and environmental impact across multiple providers to manage postpurchase flows

Disrupting your own business

The bottom line is that businesses must be willing to disrupt their own processes and models to stay ahead. This means rethinking traditional e-commerce strategies and revenue streams to embrace AI solutions that can improve product discovery, customer service, and postpurchase experiences. Of course, there will be nuances. Many consumers, after all, enjoy the experience of shopping, while others might opt for as much automation as possible. By integrating agentic AI early and investing in the right infrastructure—whether through AI-powered recommendation engines, chatbots for real-time assistance, or smart shopping assistants—businesses can gain a competitive edge by offering an increasingly frictionless, intuitive shopping journey for all their customers.

As discussed in the previous chapter, none of this will be possible without a new technical infrastructure structured around APIs that enable communication among different software systems. To facilitate smooth operations and seamless user experiences, businesses should focus on building an efficient, intuitive API infrastructure tailored to agentic needs, ensuring that AI agents can navigate the platform securely, authenticate users correctly, and manage secure transactions. And it will be crucial to build the capabilities to differentiate between a benign agent and a malicious bot. (For more on managing agentic risk and trust, see chapter 4 below.)

As AI agents increasingly influence consumer purchasing decisions, businesses must evolve to ensure their products and services are easily discoverable—not just by people, but by the agentic systems acting on their behalf. In fact, designing the "agent experience" could soon become as important a consideration as the customer experience. OpenAI took a major step in this direction with the recent announcement that it was releasing an AI-native web browser with agentic products, such as Operator, integrated into the browsing experience. This shift transcends traditional SEO, which stands to become less relevant in an agentic world. Instead, companies will need to understand and align with the data structures, preferences, and decision-making logic of AI agents—while still preserving the emotional, brand-driven experiences that build trust and loyalty with people.

> "Agentic commerce is flipping the script on how consumers engage with the digital world. We're entering an era where AI agents won't just assist—they'll decide. Business models need to evolve from optimizing clicks to earning trust from algorithms acting for consumers. This raises questions: How do you make your offering 'agent discoverable'? What does brand loyalty mean when decisions are delegated? How do you build for a world where the buyer is a model acting in someone's best interest? Leaders need to ask: Are we building experiences for people or their agents? Because increasingly, the agent will be the customer."
>
> —**Naveen Sastry,** McKinsey senior partner and global leader of software and platforms

This dual approach has the potential to unlock new revenue streams. That's because in agentic commerce, the path to purchase begins when intent first ignites. AI agents, acting on behalf of consumers, can detect and interpret early intent through contextual signals: a calendar invite for an upcoming move, a message about a new baby, or a search for homes in a new city. By engaging at this upstream moment, businesses can position themselves not just as vendors but as integral solution providers in the customer's planning process. This early access allows businesses to capture intent before a consumer even visits a product page or compares different options, effectively bypassing the traditional discovery funnel. In the case of our cross-country move, an AI agent might proactively assemble a comprehensive shopping plan: sourcing and comparing furniture options, identifying local service providers, calculating shipping costs, and optimizing timing. For those planning a vacation, an agent could preselect destination options based on calendar gaps, loyalty programs, and travel preferences.

These capabilities shift brand presence from being chosen at the point of comparison to being present at the point of need—a process with the potential to scale to thousands of micro-interactions across customers, with personalized precision and little additional human labor. The result is more efficient customer acquisition, higher conversion rates, and greater lifetime value.

Similarly, rather than relying on generic promotions, AI agents can negotiate tailored offers for customers—say, bundling furniture purchases from various retailers during a move, customized to fit budget, style, and delivery preferences. Businesses with subscription models could benefit, given the ability of agents to manage replenishable recurring purchases, whether coffee, skin care, or pet food. Real-time dynamic pricing is another potential frontier, with AI agents assessing competitors, customer intent, and inventory to propose optimal prices that maximize conversion and protect margins.

Beyond these front-end innovations, agentic AI streamlines back-end operations, from inventory planning to service automation, reducing costs and enhancing scalability. In essence, AI agents are not just a new channel; they are a catalyst for reimagining value creation and capture throughout the customer journey.

Managing risk from ad revenue decline

Of course, agentic commerce also threatens to bring about a decline in traditional revenue streams, particularly from advertising. Retail media networks, which rely on ad-based models, could face challenges as consumers shift toward agent-driven experiences that bypass traditional ad channels. Businesses will need to diversify their revenue sources and consider innovative ways to monetize through AI, such as charging for data insights or offering premium services to consumers using agents. In this evolving landscape, data from agent usage will be pivotal in guiding monetization strategies. New approaches to branding and partnerships will be essential, with potential models including affiliate-type arrangements, discovery premiums on marketing, premium placements, and subscription fees. The space is still nascent, but the following are a few examples of innovative monetization:

— *Multibrand bundling and revenue sharing.* AI agents coordinate purchases across multiple brands, bundling them into seamless experiences. For instance, when a user shops for a honeymoon package, the agent negotiates and compiles flights, hotels, excursions, and dining from different providers. Each provider receives a share of the total package fee, while the coordinating AI platform takes a service or coordination fee.

— *Real-time negotiation fees.* Agents can negotiate in real time on behalf of users, such as securing hotel upgrades or loyalty point redemptions. Platforms enabling these negotiations can charge a success fee or margin per transaction. For example, an airline might pay a fee when an agent successfully negotiates a seat upgrade.

— *Premium skills and subscription models.* Frontier labs or third-party developers can offer vertical AI agents, such as fashion stylists or upscale trip planners, through subscription plans or tiered access to advanced features and integrations, generating recurring revenue.

— *Data insights and analytics sales.* Brands can pay for anonymized, agent-filtered consumer behavior analytics to provide data on product consideration or rejection, price sensitivities, and competitor comparisons, helping brands refine marketing and product strategies.

— *Conversational marketplaces.* AI agents could evolve into full conversational marketplaces, where purchase decisions occur through dialogue. Marketplace owners monetize via brand listing fees, sales commissions, and payment-processing or protection fees.

— *Interagent protocol fees.* When AI agents from different platforms interact, monetization can happen through protocol-level fees for interoperability or commission sharing when joint value is created.

— *Contextual sponsorships in connected devices.* Brands can sponsor contextual experiences through integrations with wearables, autos, or smart homes. For example, Tesla might pay to be the default electric-vehicle provider for AI-planned trips, or Spotify could sponsor music during AI-curated events.

— *Sponsored, context-aware suggestions.* While direct advertising can compromise consumer trust, subtle "sponsored smart suggestions" aligned with user intent can be monetized, provided the agent maintains impartiality to preserve user trust.

First-movers have the unique opportunity to set and define these pricing models, capitalizing on the current monetization gaps where agents are often free and providers have yet to develop a clear revenue strategy.

Finally, as companies rethink their business models, they should proceed with the understanding that success with AI also necessitates a fundamental rewiring of organizations and the empowerment of employees. Fortunately, while leaders often cite employee readiness as a barrier to AI adoption, McKinsey research shows that employees are more prepared than their C-suite leaders believe.[14]

[14] "Superagency in the workplace: Empowering people to unlock AI's full potential," McKinsey, January 28, 2025.

CHAPTER 4

Navigating trust and risk: Why responsible AI is key to agentic commerce adoption at scale

In this evolving landscape of agentic commerce, trust transcends mere consumer sentiment. It becomes foundational infrastructure—and it will likely come under significant pressure.

The trust equation

When a person walks into a store, the trust equation is straightforward: Do I trust this brand, this merchant, this product? However, when an AI agent shops on your behalf, trust becomes abstract, filtered through layers of data, automation, and institutional frameworks. This shift prompts a profound question: Who do we trust when we aren't the ones making the choices?

For many consumers, the answer might simply be, "no one." In countries like Germany and Japan, for example, consumers still prefer traditional payment methods—such as invoices or buy now, pay later (BNPL) options—over credit cards, which tend to drive e-commerce globally.[15] Instead, account-to-account transfers dominate in Germany, accounting for 26 percent of e-commerce payments, alongside a notable 20 percent via BNPL. This shows a clear preference for methods that emphasize control and transparency. In such environments, agentic transactions might indeed be a leap of faith too far. If consumers are already hesitant to share their banking details with a static website or even a familiar payment platform, how likely are they to entrust an AI bot with not only payment credentials but also the decision-making process that leads to a purchase?

[15] *Global payments report 2025*, Worldpay, March 11, 2025.

“Getting AI trust right is a shared responsibility between the organizations deploying AI and the platform providers, governments, international organizations, and standards bodies aiming to ensure that AI is safe and reliable. In this dynamic environment, academic researchers, open-source communities, and developers also play a big role in building AI that is more trustworthy, transparent, and explainable. CEOs and CTOs can do their parts by getting their data houses in order, empowering teams to innovate safely, and monitoring all AI deployments for signs of bias or misinformation.”

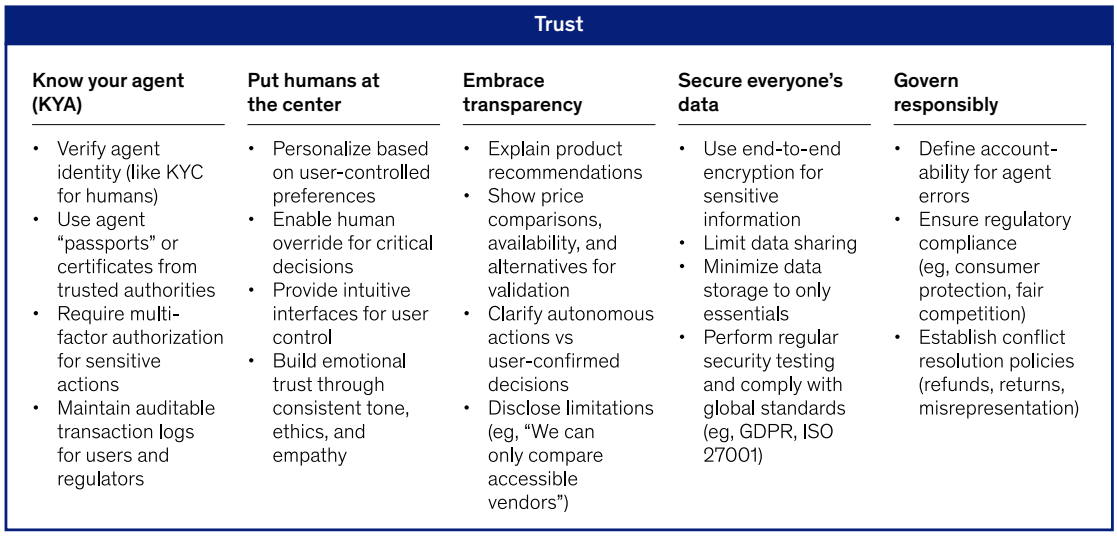
—**Roger Roberts,** McKinsey partner and global leader of the Digital Trust service line

Trust, in other words, is deeply contextual. What feels intuitive in Seoul might be unthinkable in São Paulo. Adoption doesn’t necessarily follow innovation; it follows comfort, norms, and credibility. For agents to earn trust, they should be built around people, not just processes. That means technologists must meet users where they are—not just with legal disclaimers, but with clear, ongoing dialogue. Trust, after all, is not a one-time agreement; it grows through interaction (Exhibit 5). Users should be able to ask: How is my data being used? What does this choice mean for me? They should also be able to define the boundaries of that trust. If agents are truly tools, users need intuitive ways to express and define what they’re comfortable with, preferences that the system can understand and respect. Consent, in this context, cannot be a checkbox; it must be a living, flexible agreement—one that is deepened and shaped by the user through agent–user interactions.

Exhibit 5

In agentic commerce, trust is a multilayered phenomenon comprising five dimensions.

5 dimensions of trust in agentic commerce



McKinsey & Company

The risk landscape of agentic commerce

If trust serves as the foundation of agentic commerce, then risk acts as the architecture's stress test. Trust encourages participation, while risk delineates the boundaries of that engagement. As agents gain autonomy—operating across systems, borders, and industries—new risks emerge that traditional compliance frameworks and tech governance are ill-prepared to address. Organizations should consider the following three key areas of risk:

Systemic risk: The snowball effect. Autonomous agents are more than just interfaces; they are decision-makers. Decision-making at scale introduces systemic risk, where a single faulty prompt can trigger a cascade of unintended consequences—an incorrectly booked flight, overordered inventory, a purchase that occurs without consent. When agents are interconnected across multiple systems, minor errors can have exponential impact, and resilience becomes a crucial design principle. Do agents fail gracefully? Can they backtrack? How can businesses repair reputational damage caused by a nonhuman error?

Accountability: Navigating a legal gray zone. When an AI agent makes a poor decision, determining accountability is complex. Who is to blame for that faulty transaction? The platform that developed the model? The brand that deployed the agent? The user who approved it? Currently, there is no global consensus on responsibility. The European Union's AI Act provides some clarity for high-risk systems, but enforcement is still evolving. In the United States, fragmented regulations leave companies navigating a liability vacuum. Until clearer frameworks emerge, overdisclosure and caution may be the safest approach—though this can stifle innovation, especially for start-ups lacking extensive legal resources.

The ambiguity of accountability is not just theoretical; it has commercial, legal, and reputational implications. For example, if an AI agent books a trip that gets canceled, who is responsible? The travel site? The agent? A malfunctioning third-party plug-in? Mistakes by agents can lead to brand liability, regulatory scrutiny, and systemic risk. Companies integrating agents face the challenge of aligning decision-making autonomy

with explainability. Consumers need to understand not only what an agent did but also why. Explainability is likely to become a consumer right, and auditable logs may soon be a regulatory requirement. Companies are preparing by incorporating permissions layers, identity mapping, and tiered trust levels—known as the "TRiSM" stack (trust, risk, and security management). But technical solutions alone are insufficient; the deeper issue is legitimacy.

Data ownership: A geopolitical challenge. Because AI agents operate on data, the issue of data sovereignty becomes increasingly geopolitical. Countries such as India and France are drawing firm lines with data localization efforts; Europe is seeing calls for "AI sovereignty." This raises critical questions: If an agent processes EU citizen data via a US-based API, is it compliant? If it is trained on global data but acting locally, is it lawful? While AI councils, cross-border frameworks, and watchdog coalitions are emerging, global standardization is lacking. Until such standards exist, the risk is not just technical; it's political. Regulations like Europe's General Data Protection Regulation and the EU AI Act signify a shift in data management and control, with regions focusing on digital sovereignty or innovation and risk management. OpenAI's "for countries" model, offering localized infrastructure and regulatory flexibility, highlights the challenge of scaling agentic platforms without breaching national data protection, tax, and consumer protection laws.[16] What's more, when consumers use agents powered by globally trained models, the question of legal protection arises, and the answer remains unclear. For agentic commerce to fulfill its promise, trust must be integral to its architecture. This will require transparent decision trails, fail-safes, reversibility, and regional customization of behavior and ethics to ensure agents align with user values. The combination of novelty and perceived risk often amplifies user concerns, making it essential to invest in clear communication, transparency, and the ability to safely test and explore AI systems.

Risk is not the opposite of opportunity

Finally, agentic commerce also introduces a novel kind of risk: the risk of the unknown. As agents learn to reason, improvise, and self-chain actions, emergent behaviors become possible. What is helpful today could be harmful tomorrow. Even minor shifts in how agents interpret intent could lead to subtle manipulation, adversarial exploits, or unintended amplification of bias. The question is no longer, "Is the agent safe today?" but rather, "Is the system prepared for what the agent could become?"

Every innovation, of course, brings exposure to new risks. Delivering on the promise of agentic commerce will not be about eliminating risk; it will mean learning to manage it faster than it evolves. For businesses, this means building not just for scale but for containment. For regulators, it means shifting from reaction to anticipation. And for consumers, it means demanding the same level of accountability from the systems acting on their behalf as they once demanded from people.

[16] "Introducing OpenAI for countries," OpenAI, May 7, 2025.

CHAPTER 5

The challenges and opportunities of agentic commerce

The potential of agentic commerce is immense, with the power to fundamentally transform how businesses and consumers interact. However, this transformation is not without its hurdles.

Progress toward capturing the projected $3 trillion to $5 trillion economic opportunity will depend heavily on how effectively these challenges are addressed. Companies must navigate the intricate task of integrating AI into existing systems, uphold rigorous standards of data privacy, and adapt to fast-evolving consumer expectations. To fully unlock the potential of agentic AI, organizations should address a series of critical strategic and operational questions across three key domains.

"The transition from static e-commerce to a more dynamic agentic commerce system unlocks transformative potential, redefining customer experiences and operational agility. To thrive in this era of autonomous digital commerce, businesses must act now, as AI is already changing the way we interact. Investing in agent-ready infrastructure—encompassing APIs, data interoperability, trust frameworks, and governance—is essential to staying competitive in a rapidly evolving landscape."

—**Lari Hämäläinen,** senior partner and global gen AI and agentic services lead at QuantumBlack, AI by McKinsey

Capabilities, go-to-market strategy, and brand

The following questions can help organizations form the basis for a strong competitive position as they develop their agentic commerce strategies.

First-mover advantage. How can your business swiftly gain a first-mover advantage and build a defensible moat through strategic API development and AI partnerships? Identifying the prerequisites, such as robust tech infrastructure and a modular partnership ecosystem, will be essential for adapting to shifts in consumer behavior.

Scaling AI competitiveness. What strategies will enable your business to ramp up in the next two to three years to effectively compete with AI tools? With no single dominant AI player, businesses need to approach AI partnerships with adaptability in mind.

Proprietary versus partnership. To what extent should your business develop proprietary AI solutions versus exclusively partnering with AI developers? Consider the type of partners needed to build a future-proof ecosystem that creates a unique selling proposition in an agentic AI world.

Evolving work practices. How will your operations evolve in the era of AI? Transitioning from an isolated "AI team" to embedding AI across all teams, similar to the mobile shift, will be critical for success.

Brand differentiation. How can you differentiate and strengthen your brand in a landscape where AI increasingly handles customer interactions and decision-making? Understanding what brand identity looks like in a future dominated by AI and automation is crucial.

Concierge experience. How can your businesses create a unique and personalized concierge experience in an era where AI agents are central to customer interactions? Crafting a truly distinct concierge service through AI can drive customer satisfaction and loyalty and set the brand apart in a competitive market.

Monetization strategies

Agentic commerce potentially threatens existing revenue streams. The following questions can help leaders mitigate those disruptions—while they seek to capitalize on new opportunities the technology presents.

Innovative revenue models. As AI disintermediates traditional revenue streams like ad revenue, what innovative revenue models can your business create? Leveraging AI to offer value-added services, premium offerings, or new products that customers are willing to pay for is key.

Data monetization and personalization. What role can data monetization, AI-powered personalization, or subscription-based models play in generating new streams of revenue? Agentic AI can enable your business to capture an even broader share of the wallet.

Trust and risk

In addition to opening new opportunities, agentic commerce also presents novel risks, especially regarding customer trust and relationships. The following questions can help leaders understand the potential risks they might face.

Consumer trust. How can your business earn and preserve consumer trust when delegating decisions to autonomous agents? Clear communication, transparency, explainability, and human override features can help build confidence, but local culture influences both trust and adoption.

Trust transferability. Will consumers trust agents simply because of the brands deploying them? Understanding the limits of brand halo effects, and knowing when users need proof of safety, reliability, or explainability, will be essential.

Data sovereignty. How does the movement of data across borders impact user trust in agentic systems? Consumers and local governments might demand stronger assurances of local data handling, auditability, and ethical oversight.

Systemic risk. What guardrails are needed to prevent cascading failures across interconnected agents and ecosystems? Building resilient, modular architectures and fail-safe protocols will define the maturity of agentic infrastructure.

Adoption. Will agents ever be widely adopted in markets with low digital payment penetration or institutional trust? Adapting agent behaviors to local trust norms and offering layered human control will be essential for global scalability.

Admittedly, this is a lot to consider. But leaders who embrace this moment with vision and courage will find themselves at the forefront of a new era. They will see beyond the risks of disruption to the possibilities of reinvention. They will recognize that the future of commerce is not about replacing human ingenuity but amplifying it—with systems where AI and humans work in harmony to deliver great experiences and great value. Businesses that act now—investing in flexible architectures, experimenting boldly, rethinking their models, and aligning with their customers' desires and preferences—can not only adapt to this new reality but shape it.

Katharina Schumacher is a partner in McKinsey's Munich office, and **Roger Roberts** is a partner in the Bay Area office, where **Katharina Giebel** is a consultant.

The authors wish to thank Becca Coggins, Deepa Mahajan, Eli Stein, Hannah Mayer, Lareina Yee, Lari Hämäläinen, Marie-Claude Nadeau, Naveen Sastry, and Vikram Iyer for their contributions to this report. They also wish to thank Mara Pometti and Sophie Marchessou for their insights.

This report was edited by Larry Kanter, a senior editor in the New York office.

This report contributes to McKinsey's ongoing research on AI and aims to help business leaders understand the forces transforming ways of working, identify strategic impact areas, and prepare for the next wave of growth. As with all McKinsey research, this work is independent and has not been commissioned or sponsored in any way by any business, government, or other institution. The report and views expressed herein are ours alone.

We welcome your comments on this research at agenticcommerce@mckinsey.com. Learn more about our gen AI insights and sign up for our newsletter.

October 2025

Designed by McKinsey Global Publishing

www.McKinsey.com