



Future of payments

Insights for 2027

Contents

Executive summary	3
Trend 1: AI in the hands of bad actors: Risks accelerated by real-time payments and agentic commerce	4
Trend 2: The rise of bot shoppers: Agentic AI transforms digital commerce	6
Trend 3: Money that moves itself: AI agents augment impact of digital payments	8
Trend 4: The responsibility gap: Embedded finance momentum builds the case for stronger governance	10
Trend 5: New payments gatekeepers: Big Tech reshapes financial services	11
Conclusion	12
Contacts	13

Executive summary

The payments landscape continues to be sculpted by artificial intelligence (AI), real-time payments, digital assets, and evolving regulatory expectations. Last year, we predicted that the regulatory and economic environment would take the brunt of the impact, while this year the effects are elevating to direct customer impact and landscape shifts. That shift is already underway: Last year's stablecoin and agentic-AI pilots have moved into live deployment, and agentic commerce is starting to reshape who initiates a payment in the first place. Banks, payment networks, fintechs, and merchants should consider the challenges that exist from watching from the sidelines. The institutions that move first to build trust, controls, and agentic-ready infrastructure will define this new era, while those that wait risk ceding the customer relationship to those who move faster.

Deloitte developed predictions for the future of payments in 2027 across five areas:

1. AI in the hands of bad actors: Risks accelerated by real-time payments and agentic commerce

AI is enabling faster, harder-to-detect fraud across the customer journey, from synthetic identities at onboarding to scams exploiting real-time payment rails. The real shift is upstream: Financial institutions are moving fraud defense to the point of identity validation, combining biometrics, tokenization, and consumer education, before a transaction is ever attempted.

2. The rise of bot shoppers: Agentic AI transforms digital commerce

Agentic commerce is moving from concept to production. Shopping assistants are already being demoed and folded into existing retail experiences, even as fully native, agent-led storefronts remain early. Adoption is climbing even as consumer comfort with AI-led purchasing is falling, so success will likely depend on designing experiences for both human customers and AI agents while providing the transparency, controls, fraud protection, and accountability consumers need to confidently delegate purchasing power.

3. Money that moves itself: AI agents augment impact of digital payments

For autonomous agents to transact at scale, they need money that can move as fast and as programmatically as they do. Stablecoins, tokenized deposits, and agentic AI are converging to enable programmable, always-on payments across business, consumers, and technology. As multiple settlement rails emerge, financial institutions will need to determine where each creates strategic value while building common authorization and spending controls to work across them.

4. The responsibility gap: Embedded finance momentum builds the case for stronger governance

The rapid expansion of embedded finance is exposing potential gaps in accountability across banks, fintechs, and tech providers as US oversight remains fragmented. The Synapse collapse illustrates why financial institutions must proactively strengthen governance and third-party oversight, rather than rely on regulation alone to determine responsibility.

5. New payments gatekeepers: Big Tech reshapes financial services

Big Tech's evolving payments strategy increasingly centers on owning the customer interface while relying on regulated financial institutions to provide underlying infrastructure and manage financial risk. As agentic commerce scales, that interface position increasingly means owning the layer that verifies an AI agent's identity and authority to transact, encroaching on banks and payment networks' current control. This creates both competitive pressure and partnership opportunities for institutions that can differentiate through trust and regulatory risk management.

Together, these trends point to a broader transformation afoot: Payments are becoming increasingly intelligent, autonomous, and embedded into everyday experiences, while trust and accountability become more critical. Banks, payment networks, fintechs, and merchants who lead in this next era will need to move beyond framing payments solely as transaction processing. They will need to begin experimenting with new capabilities and business models while strengthening the controls, governance, and customer confidence required to scale them.

TREND 1: AI IN THE HANDS OF BAD ACTORS

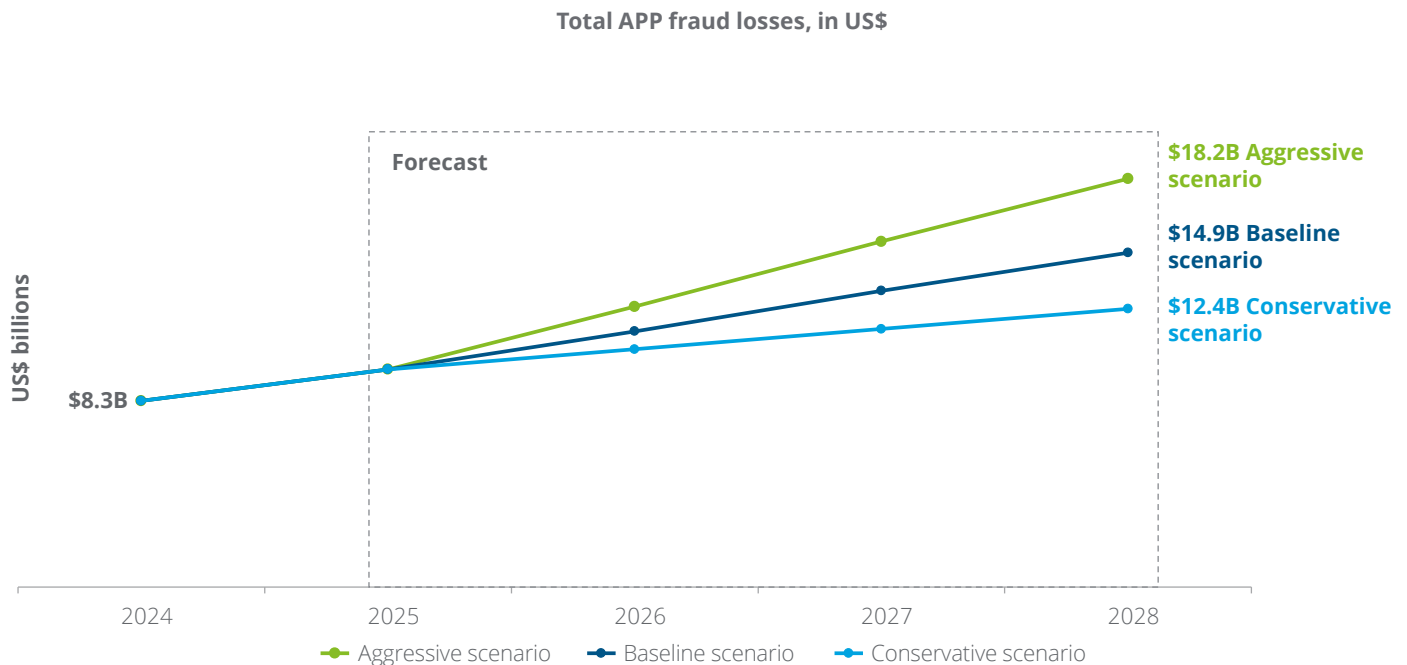
Risks accelerated by real-time payments and agentic commerce

As generative and agentic AI evolve and instant payments gain traction, financial institutions are moving fraud defense upstream, from a single checkpoint at the moment of payment to continuous validation of identity and intent across the entire customer relationship.

Synthetic identity fraud is becoming more frequent and sophisticated during customer onboarding, as digital interactions expand and generative AI advances. The financial impact is significant: Deloitte anticipates synthetic identity fraud to generate at least \$23 billion in losses by 2030. As dark-web data and generative AI make fabricated

faces, documents, and voices easy to produce, financial institutions need stronger ways to distinguish legitimate applicants from fraudsters. Combining behavioral biometrics with physical biometrics can strengthen onboarding defenses by helping confirm that a real person is opening the account.¹ These tools can also enhance login controls. For example, screening the pace of password entry or navigation on a mobile application can inhibit cybercriminals. Visa's pending \$2.4 billion acquisition of BioCatch, a behavioral biometrics provider, signals how central this kind of continuous, session-level signal is becoming to fraud prevention.²

Figure 1. Losses due to authorized push payment fraud are expected to grow in the United States no matter the scenario



Note: 2026–2027 values interpolated between the report's labeled 2024 actual and 2028 forecast endpoints for chart continuity.

Source: Federal Trade Commission's Consumer Sentinel Network US consumer fraud data and Deloitte Center for Financial Services analysis and forecast.

At the time of transaction, agentic commerce complicates the payment authorization landscape. AI agents are now not only helping buyers search for products but also completing purchases on behalf of consumers or businesses, sometimes without any human interaction. As agents increasingly act on a buyer's behalf, merchants and issuers need new ways to verify that a transaction reflects the consumer's identity, intent, and authorized instructions. One example response is Mastercard partnering with Google on "Verifiable Intent," a trust layer specifically designed for agentic commerce, which creates a record of consumer identity and authorization/instructions to support consumers, merchants, and issuers including in the case of disputes.³

In parallel, the shift from pull-based to push-based payments increases the stakes of fraud controls as fraudsters gain immediate access to stolen funds. Once funds move, real-time push payment rails leave little room for recovery. Deloitte estimates that US losses from authorized push payment (APP) fraud could surge to nearly \$15 billion by 2028 (figure 1), with AI-enabled investment scams, bank/business impersonation, and romance imposter scams driving the bulk of that growth.⁴ As fraudsters become faster and more convincing, financial institutions should shift focus from recovering losses after the fact to real-time signals, such as device and behavioral biometrics and confirmation-of-payee checks, that flag a payment as suspicious before authorization completes.

To combat fraud risk amidst these advancing technologies, institutions need a layered response combining credential modernization, consumer education, and embedded fraud-control features built directly into platforms such as confirmation-of-payee at authorization. Regulators are signaling they won't wait for the payments industry to close this gap on its own timeline. For example, the United Kingdom's mandatory reimbursement rule for APP fraud victims is an early example of regulation stepping in ahead of industry-led fixes; the rule, which has been in effect since October 2024, splits fraud costs evenly between sending and receiving institutions and requires refunds within five business days, which supplements confirmation-of-payee checks and cross-industry coalitions such as Stop Scams UK.⁵

Although banks in the United States are generally not required to reimburse for APP fraud associated with authorized payments, the loyalty of their customers may depend on keeping up with fraud control innovation and effectively identifying the sources of fraudulent activity. For example, a study in the *Production and Operations Management* journal found that attrition substantially increases for customers impacted by fraud when a bank does not share a clear answer on the cause of fraud. On the other hand, if the bank successfully catches the fraudster, impacted customers are more likely to stay with the bank than customers who have not been affected by fraud.⁶

To keep pace with the AI-driven evolution of fraud tactics, organizations across the payments landscape will likely need to strengthen controls across the customer journey, from onboarding through money movement. Together, these measures shift fraud defense upstream, moving beyond transaction-level fraud detection to build a persistent view of each customer's identity, enabling payments companies to detect fraud earlier and more accurately.

TREND 2: THE RISE OF BOT SHOPPERS

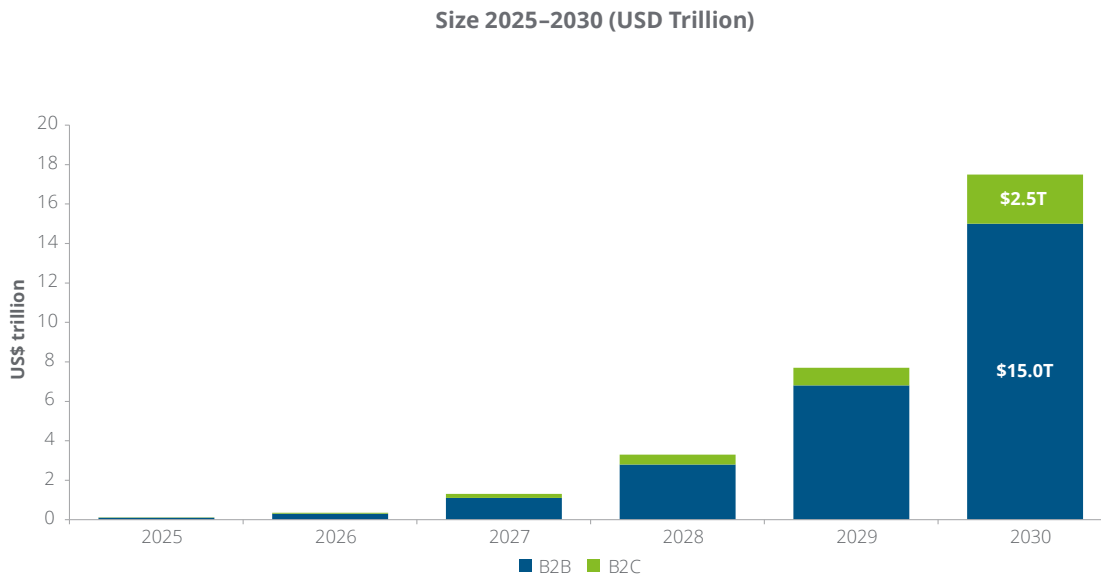
Agentic AI transforms digital commerce

The same agentic capabilities that widen fraud's attack surface are also opening an entirely new channel for legitimate commerce and reshaping who the customer actually is. Consumer-facing personal-assistant apps, many of which already hold payment and preference data, are positioned to play a meaningful role here too, though it is not yet clear whether all of them meet Payment Card Industry (PCI) compliance standards. AI agents are rapidly evolving from recommendation resources into autonomous purchasing assistants capable of researching products, comparing prices, negotiating offers, and completing transactions on behalf of consumers. Adoption is moving faster than most merchants can prepare. Global survey data shows nearly three in four shoppers (73%)⁷ are using AI at some point

in their shopping journey, and Visa research finds almost half of US shoppers (47%)⁸ now use AI tools for shopping support, including price comparisons and personalized recommendations. That headline number is mostly ambient adoption of AI-assisted recommendations and comparisons consumers don't think of as agentic, rather than shoppers who have handed a purchase decision to an agent outright, and the gap between the two is growing.

As these agents become increasingly adopted, they will likely influence a growing share of digital commerce decisions, changing how consumers discover and purchase products. Payment networks and technology providers are already developing authentication

Figure 2. Agentic AI influenced gross merchandise value



Source: Deloitte, The Future of Commerce in an Agentic World: How Agentic AI Will Reshape Commerce & What Payment Networks Must Do Next (Deloitte Development LLC, 2025), based on a survey of 500+ consumers and businesses. GMV and transaction-value figures are Deloitte Estimates and Commerce Tools data cited therein; business-willingness figure from the same survey.

standards and protocols designed specifically for AI-driven transactions, laying the foundation for an emerging ecosystem of agent-to-merchant commerce.

The next generation of commerce will require businesses to design marketplace experiences for both human customers and AI agents acting on their behalf. Merchants may need to rethink digital storefronts, pricing transparency, application programming interfaces (APIs), authentication, and loyalty strategies to ensure they remain discoverable and preferred by autonomous shopping agents.

The scale of this shift is substantial: Agentic AI is projected to enable \$17.5 trillion in gross merchandise value by 2030 (figure 2), with roughly 30% of digital commerce transaction value influenced by AI agents by that point.⁹ Half of businesses surveyed say they would work with autonomous agents to improve efficiency and personalization.¹⁰

Despite the projected growth, consumer sentiment on agents has reversed: While 70% of consumers in 2025 expressed some comfort with AI agents making purchases, in June of 2026, a majority (55%) are now uncomfortable with that level of autonomy.¹¹ Concerns were cited around AI making poor decisions or taking unauthorized action (57%), security and data-privacy risk (58%), and reliability or accuracy of agent outputs (39%).¹² Consumers also noted what would change their minds: guaranteed reimbursement for AI-related errors paired with the ability to review and override agent actions (59% want this), full control over where and how agents can act (57%), and real-time notifications and transparency into agent decisions (37%).¹³ Consumers who feel financially secure are roughly three times as likely to be comfortable with agentic AI in their finances as those who feel financially insecure (32% vs. 10%), indicating that a single playbook for building customer trust may not land the same way across every segment.¹⁴

The broader consumer credit backdrop reinforces why that segmentation matters. US credit card delinquencies eased to about 2.9% in the first half of 2026, down from a 2024 peak near 3.2%; charge-offs decreased to 3.8% of balances, total credit card debt reached \$1.25 trillion, and serious auto-loan delinquency hit 5.5%, above the level seen during the 2008–09 financial crisis.¹⁵ That is not a consumer in crisis, but it is not a consumer with much slack either.

Financial institutions should not wait for consumer trust to catch up to adoption. There is a usage-versus-confidence gap that will likely keep growing before it narrows, and it will not resolve into a single customer segment: It will split by degree of financial security, tech comfort, and the controls an institution provides, so a single trust playbook will not land the same way for every user. Institutions and merchants that address the control and trust piece directly, with a best-in-class agentic experience founded on visible fraud protections, transparent AI disclosures, and clear accountability, will be well-positioned to transform digital commerce. Those that don't may find their agentic commerce investments underutilized.

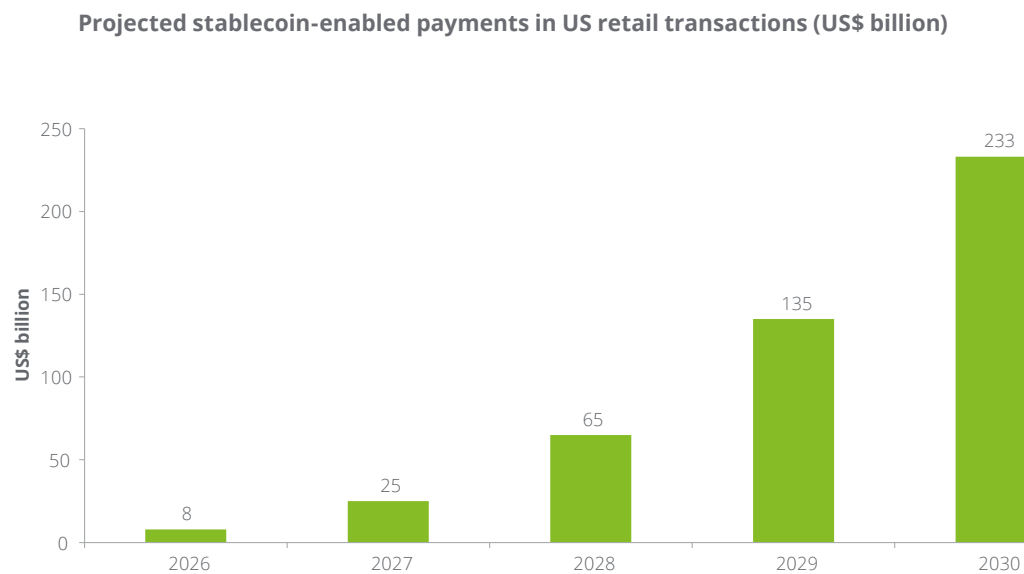
TREND 3: MONEY THAT MOVES ITSELF

AI agents augment impact of digital payments

Stablecoins, tokenized deposits, and agentic AI are converging to create an always-on payments ecosystem capable of moving money autonomously across consumers, businesses, and machines. Stablecoins enable instant, programmable, cross-border settlement; tokenized deposits offer that same speed and programmability while preserving the benefits of a bank deposit. AI agents add the ability to initiate and manage payments on either rail within defined policies and controls.

The passage of the GENIUS Act last year marks an important turning point by providing a regulatory framework that could accelerate enterprise adoption and give financial institutions greater confidence to invest in stablecoin-enabled payment capabilities. The stablecoin market has grown roughly 30fold since the beginning of 2021 to about \$300 billion in circulation,¹⁶ and Deloitte projects more than \$200 billion of US retail payments will be stablecoin-enabled by 2030, with agentic shopping a leading catalyst.¹⁷

Figure 3. Stablecoins could underpin a growing share of US retail commerce through 2030



Source: Deloitte Center for Financial Services analysis of US Census Bureau data.

As policymakers seek to provide greater regulatory clarity, financial institutions should shift focus from whether these tools matter to where each creates strategic value. Increasingly, that value depends on who, or what, is initiating the payment. An increasing number of transactions are now initiated by an autonomous agent, not a person. For example, x402, an open protocol that lets AI agents pay each other in stablecoins for machine-native purchases like API calls and compute, has processed more than 178.3 million agent-initiated transactions since its launch in May 2025.¹⁸ This changes what has to happen before money moves: An agent decides what it wants and negotiates with a merchant, and a control layer verifies its identity and checks the request against a scoped mandate, spending limit, and expiry before authorizing it. Only then does settlement execute. Product discovery and negotiation of the payment are standardizing fast on competing protocols and “shop for me” retail assistants. Settlement of these agentic transactions already runs three lanes: cards for everyday consumer purchases, stablecoins for external payments too small to be viable for traditional payment methods or where programmability is required, and tokenized deposits for settlement that stays inside the paying institution. Authorization sits in between discovery and settlement, with compliance built into the mandate itself rather than reviewed after the fact. This piece of the landscape remains contested, with card networks, banks, and fintechs all racing to define the standard in order to capture customer relationship, no matter which lane settles the transaction.

Trust, not technology, is what’s actually gating adoption at that authorization step. Deloitte’s own Stablecoin & Agentic Commerce Survey of more than 1,500 US consumers and business leaders found banks the trust leader, chosen by 75% of consumers and 46% of business leaders over any fintech alternative, while fraud and scam concerns remain the top barrier.¹⁹ For agentic payments specifically, both audiences want the same thing: approval rights, spending limits, and clear accountability when something goes wrong.

That same compliance-first logic applies to how the money actually moves, too. A tokenized deposit gives a bank the same programmability and near-instant settlement as a stablecoin without moving cash off its balance sheet or out of its lending base. A stablecoin doesn’t, even one the bank issues itself: Under the GENIUS Act, stablecoin issuers can’t pay interest, and their reserves have to sit in safe and liquid assets rather than loans, so every dollar that converts into one is a dollar the bank can no longer lend against. JPMorgan has already made this real: Its Kinexys platform, which offers a tokenized deposit rail known as JPM Coin, processes about \$7 billion in transactions daily.²⁰ Internationally, Swift, the organization that

helps banks communicate and move money around the world, is trying something similar. In July 2026, Swift started testing a blockchain-based system with 17 banks. The system uses digital versions of bank deposits to help banks send and settle money with each other 24/7, instead of moving money only within one bank.²¹

Primary use cases are live today: cross-border payments, automated treasury management, always-on settlement, and dynamic supplier payments. Emerging use cases lean further into agentic territory: microtransactions too small for a card network to support, escrow and programmable payments, and scalable machine-to-machine commerce. These apply wherever rules-based decisioning meets programmable financial rails, and increasingly there are multiple rails to choose from.

Now is the time to move from observation to experimentation. Merchants should assess where stablecoins and agentic commerce improve conversion and cost. Banks and issuers should build one strategy for tokenized deposits and stablecoins, not two, with both carrying verifiable agent identity and spending limits from day one, starting with regulated issuance and institutional settlement. Payment networks and payment service providers should compete on cross-rail identity and authorization, not on which currency settles. Risk and compliance should move controls from periodic review into the transaction itself. Corporate treasury should pilot one bounded, agent-initiated flow now, before volume makes mistakes expensive. Companies should also explore instant sweeps that move idle stablecoin balances, which earn nothing on their own, into a yield-bearing product, a tokenized money market fund or DeFi staking, and back again the moment the cash is actually needed. Early movers will shape the customer experience and the operating standard; everyone else will compete on infrastructure someone else already built.

TREND 4: THE RESPONSIBILITY GAP

Embedded finance momentum builds the case for stronger governance

As settlement increasingly spans banks, fintechs, and technology intermediaries in pursuit of that always-on model, a harder question follows the money: When something breaks mid-chain, who will answer for it? In April 2024, Synapse Financial Technologies, Inc., a technology and ledger service provider connecting fintech apps with Federal Deposit Insurance Corporation (FDIC)-insured banks, collapsed after disputes with partner banks and a major client exposed gaps between its internal records and actual bank balances. The collapse left more than 100,000 people without access to over \$265 million held across several fintech platforms.²² Most customers assumed FDIC insurance covered them, but FDIC insurance protects against a bank's failure, not the failure of the intermediary provider routing money to that bank.²³ No one could say with certainty who was responsible among the bank, the intermediary provider, and the fintech app.

The gap between how fast embedded finance is scaling and how equipped regulation is to assign accountability is growing. US embedded finance revenue is projected to hit \$51 billion in 2026, up from \$40 billion in 2025, moving roughly \$7 trillion in transaction volume.²⁴ Synapse exposed an accountability question the industry still hasn't answered. Money transmission is regulated almost entirely at the state level, with 49 states and Washington, D.C. running separate licensing regimes, with no single federal charter covering embedded finance nationally. California's Digital Financial Assets Law took effect on July 1, 2026, adding another state-specific standard on top of that patchwork.²⁶ The result is more than 50 jurisdictions defining oversight differently; banks should treat the strictest state standard as their floor, because retrofitting compliance after a failure costs more than building to it up front.

At the federal level, the Consumer Financial Protection Bureau (CFPB) has rescinded nearly 70 interpretive rules, policy statements, circulars, and advisory opinions, since 2025²⁶ including guidance that had let fintechs seek up-front compliance approval through no-action letters and regulatory sandboxes.²⁷ Moreover, the CFPB proposed a rule in 2025 that would cut nonbank supervision, impacting a substantial number of firms.²⁸

Even banks that benefit from lighter nonbank compliance costs are flagging the risks associated with updates to interpretive rules and policy statements. Banks should not read these types of changes as license to loosen their own third-party oversight, as it raises, rather than lowers, the bar for compliance.

Conversely, the UK offers other models. As an example, the appointed representative regime gives regulators a clearer basis for holding the authorized principal firm responsible for the regulated activities carried on by its appointed representative within the scope of the appointment, supported by ongoing oversight obligations.²⁹

Synapse illustrates why embedded-finance risk must be managed across governance and accountability, resilience, customers, and data rather than through licensing alone.

Some firms are choosing not to manage that risk but to exit it. Revolut currently serves US customers through FDIC-insured bank partners rather than its own charter. That is the same kind of fintech-to-bank dependency that left Synapse's customers exposed when the intermediary's own records diverged from what its partner banks held. Revolut says a national bank would let it serve customers more cheaply and efficiently than that model allows. It filed for the charter on March 10, 2026, and received conditional Office of the Comptroller of the Currency (OCC) approval in September, though the OCC withheld four of the products it requested pending further review.^{30,31} Nubank, which has no existing US operation to convert, moved faster. It filed in September 2025 and received conditional approval in January 2026, in just 121 days.^{32,33}

For payments specifically, the charter question decides who holds settlement risk and reconciliation liability once a fintech's volumes get large enough to matter—the same responsibility gap Synapse exposed, just resolved by absorbing the liability directly instead of routing it through a partner bank.

Financial institutions should act proactively across these four domains rather than wait for a failure to impose it: maintain independent, real-time reconciliation with every fintech partner's ledger; assign clear contractual liability before onboarding a partner, not after a dispute; and treat state-level licensing as a floor rather than a checklist to clear. Liability in embedded finance is not a compliance footnote; it is what determines whether a firm controls its own risk or has it decided for them.

TREND 5: NEW PAYMENTS GATEKEEPERS

Big Tech reshapes financial services

By 2027, expect Big Tech to compete less on transaction volume and more on owning the single moment that verifies an AI agent's identity and authority to transact, the next chokepoint in payments. Big Tech's payments strategy is itself a live case study in that same responsibility gap: Technology platforms are moving fastest to own the customer interface, while working to ensure regulated partners retain the risk and compliance burden. As Big Tech's core competencies reach saturation points,³⁴ they have ventured into the payments industry. Tech's foray into the payments space has followed a market penetration approach that traditionally proved successful, leveraging their existing customer relationships to drive adoption of their proprietary tech. Big Tech's expansion into financial services has evolved to own the interface and let a regulated partner own the risk. Understanding this shift, and positioning accordingly, is essential for payment providers and banks looking to remain competitive in the payments space.

Tech platforms control many of the customer touchpoints that define modern payments through digital wallets (83% of digital payments are made today via digital wallets),³⁵ consumer devices, and identity services. With access to extensive behavioral data and trusted consumer relationships, these companies were well positioned to expand into adjacent financial services.

Tech companies encountered complexity when also acting as the financier, with several major players retiring platforms or changing relationships soon after inception. The largest firms launched branded credit cards,³⁶ in-house buy-now-pay-later (BNPL) services,³⁷ and proprietary cryptocurrencies.³⁸ Today, these products have been either reshaped in partnership with established payment providers, or sunsetted entirely. In comparison, Google Wallet and other digital wallet services are finding success with a push into digital driver's licenses,³⁹ letting state governments own the regulatory and risk aspects while they gain adoption.

Legacy financial institutions remain the bedrock in the payments space, but we are already in a future where they increasingly compete behind the scenes while technology platforms own the primary customer experience. Institutions should focus on demonstrating their value as a capable regulatory and risk partner with the goal of amplifying their customer base, using Big Tech partnerships as the vehicle.

Looking to 2027, expect this dynamic to sharpen around a more specific prize: agent identity and authorization. The same Big Tech platforms already building the trust layer for agentic commerce are best positioned to grow as the default verification layer that confirms an AI agent's identity and authority to transact, before a payment ever reaches a bank or issuer. If that plays out, Big Tech's payments strategy will have shifted from owning transaction volume to owning the moment of trust that authorizes it, encroaching on banks' and payment networks' current control.

The institutions that win this round won't be the ones resisting Big Tech's push into verification—they'll be the ones that make themselves the obvious regulated back end for it.

Conclusion

Underlying all five trends is one dynamic: Innovation is outrunning regulation. Institutions that want to compete for the agent-identity layer rather than be defined by it should do three things: invest in the unglamorous work of proving trust, such as reconciliation, credential modernization, and verifiable identity, before it is required of them; hold partners to the same scrutiny they would apply to their own operations, rather than treating a partnership as a

transfer of risk; and design for the customer as they actually are today, financially secure or not, comfortable with AI or not, rather than the customer institutions wish they had. Banks, payment networks, fintechs, and merchants that act on these three now will shape the operating standard for 2027. Those that wait will compete on infrastructure someone else already built.



Contacts

Tim Davis

Principal
Deloitte & Touche LLP
timdavis@deloitte.com
+1 206 716 7593

Satish Lalchand

Principal
Deloitte Transactions and Business Analytics LLP
slalchand@deloitte.com
+1 202 220 2738

Roy Ben-Hur

Managing Director
Deloitte & Touche LLP
rbenhur@deloitte.com
+1 973 602 4233

Raquel Gomez

Managing Director
Deloitte Consulting LLP
rgomezsirera@deloitte.com
+1 703 251 1052

Divakar Goswami

Managing Director
Deloitte Consulting India Private Limited
dgoswami@deloitte.com
+1 615 718 5910

Sohail Kagzi

Managing Director
Deloitte Consulting LLP
skagzi@deloitte.com
+1 703 251 4143

Neda Shemluck

Managing Director
Deloitte Services LP
nshemluck@deloitte.com
+1 415 783 6634

Tanmay Agarwal

Senior Manager
Deloitte Consulting India Private Limited
tagarwal@deloitte.com
+1 470 434 1903

Valeria Gallo

Senior Manager
Deloitte LLP
vgallo@deloitte.co.uk
+44 20 7303 6745

Menes Etingue Kum

Senior Manager
Deloitte Consulting LLP
metinguekum@deloitte.com
+1 212 436 2507

Nora Linkous

Senior Manager
Deloitte Consulting LLP
nlinkous@deloitte.com
+1 703 251 3531

Brendan Maggiore

Senior Manager
Deloitte Transactions and Business Analytics LLP
bmaggiore@deloitte.com
+1 202 370 2396

Vishal Kalsi

Associate Vice President
Deloitte Consulting LLP
vikalsi@deloitte.com
+1 212 313 1682

Endnotes

1. Val Srinivas, Satish Lalchand, and Jill Gregorie, "[Using biometrics to fight back against rising synthetic identity fraud](#)", *Deloitte Insights*, July 27, 2023.
2. BioCatch, "[Visa to acquire BioCatch](#)," press release, August 3, 2026.
3. Pablo Fourez, "[When AI starts buying for you, trust becomes the product](#)," Mastercard, March 5, 2026.
4. Satish Lalchand et al., "[Forecasting the rise of push payment scams—the fraud consumers are tricked into authorizing](#)," *Deloitte Insights*, October 9, 2025.
5. Joseph Sullivan, "[APP fraud: The UK's mandatory reimbursement requirement](#)," Thomson Reuters Institute, April 2, 2024.
6. Shannon Roddell, "[Banks that identify fraudsters increase loyalty, retain more defrauded customers than others who never were compromised](#)," Notre Dame News, September 22, 2025.
7. Or Shmueli, "[Global Study: 73% of Shoppers Using AI in Shopping Journey – But Merchants Face New Agentic Commerce Risks](#)," Riskified, October 20, 2025.
8. Visa, "[Visa and partners complete secure AI transactions, setting the stage for mainstream adoption in 2026](#)," press release, December 18, 2025.
9. Deloitte, [The future of commerce in an agentic world](#), August 2025, based on a survey of 500+ consumers and businesses. GMV and transaction-value figures are Deloitte estimates and commerce tools data cited therein; business-willingness figure from the same survey.
10. Ibid.
11. The Wise Marketer, "[Riskified study finds consumers aren't ready to hand over control as AI transforms shopping](#)," June 8, 2026.
12. Deloitte, [The future of commerce in an agentic world](#), August 2025, based on a survey of 500+ consumers and businesses.
13. Ibid.
14. Ibid.
15. Board of Governors of the Federal Reserve System (FRB), "[Charge-off and delinquency rates on loans and leases at commercial banks](#)," series DRCCCLACBS, retrieved via FRED, 2026; Matt Schulz, "[2026 credit card debt statistics](#)," LendingTree, September 11, 2026.
16. Thomas Campione, "[Stablecoins: From exploration to strategic imperative](#)," Deloitte, February 17, 2026.
17. Tim Davis and Jill Gregorie, "[How stablecoins could power the next era of retail payments](#)," *Deloitte Insights*, May 20, 2026.
18. Visa and Artemis, [Agentic payments from the ground up](#), July 2026.
19. Deloitte US, "Stablecoin & Agentic Commerce Survey," May 2026.
20. JPMorgan, "[How blockchain and digital assets have moved from pilots to production-grade commercial solutions](#)," August 5, 2026.
21. Swift, "[Swift's blockchain ledger ready for use as 17 banks set to pioneer tokenised cross-border payments on trusted global infrastructure](#)," press release, July 9, 2026.
22. Rafael Morales-Guzman, "[The Synapse collapse exposes why the world needs stronger fintech regulation](#)," *Yale Journal of International Affairs* 21, no. 1 (December 7, 2025).
23. Federal Deposit Insurance Corporation (FDIC), "[Understanding deposit insurance](#)," last updated April 1, 2024.
24. Trace Cohen, "[Embedded finance in 2026: Every company becoming a fintech, what actually works](#)," Value Add VC, July 7, 2026.
25. Jarsun, Ferreira & Calvo, "[Money transmission in the United States: Licenses, requirements, exemptions and alternatives for payment companies and fintech](#)," March 9, 2026.
26. Trace Dodge, "[The deregulatory pendulum swing: Life after a neutered Consumer Financial Protection Bureau](#)," Capstone, December 22, 2025.
27. Keith Schostag, "[Withdrawn! Sixty-seven pieces of guidance withdrawn by the CFPB](#)," America's Credit Unions, May 15, 2025.
28. Caitlin Mullen, "[CFPB proposes trimming its nonbank purview](#)," *Banking Dive*, August 26, 2025.
29. Financial Conduct Authority (FCA), "[Principals and appointed representatives](#)," accessed May 20, 2026.

30. Office of the Comptroller of the Currency (OCC), [Corporate Decision #1390](#), September 2, 2026
31. Melinda Lucy, "[Fintechs asking for, and receiving, bank charters in 2026](#)," *American Banker*, April 28, 2026
32. US Securities and Exchange Commission (SEC), [Nu Holdings Ltd. Form 6-K](#), January 29, 2026.
33. Melinda Lucy, "[Fintechs asking for, and receiving, bank charters in 2026](#)," *American Banker*, April 28, 2026
34. PYMNTS, "[Tech giants just made every business their business](#)," May 5, 2026.
35. Sofia Ramirez, "[Digital wallet statistics 2026: What's surging now](#)," *SQ Magazine*, February 9, 2026.
36. Apple, "[Chase to become new issuer of Apple Card](#)," January 7, 2026.
37. PYMNTS, "[Apple shuts Pay Later, paving new path for installment loans](#)," June 17, 2024.
38. Iulia Musat, "[Meta reported to be planning stablecoin payments integration in second half of 2026](#)," *The Paypers*, February 25, 2026.
39. Credence ID, "[Mobile driver's license issuing-state tracker 2026](#)," last updated March 2026.



Together makes progress

As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.