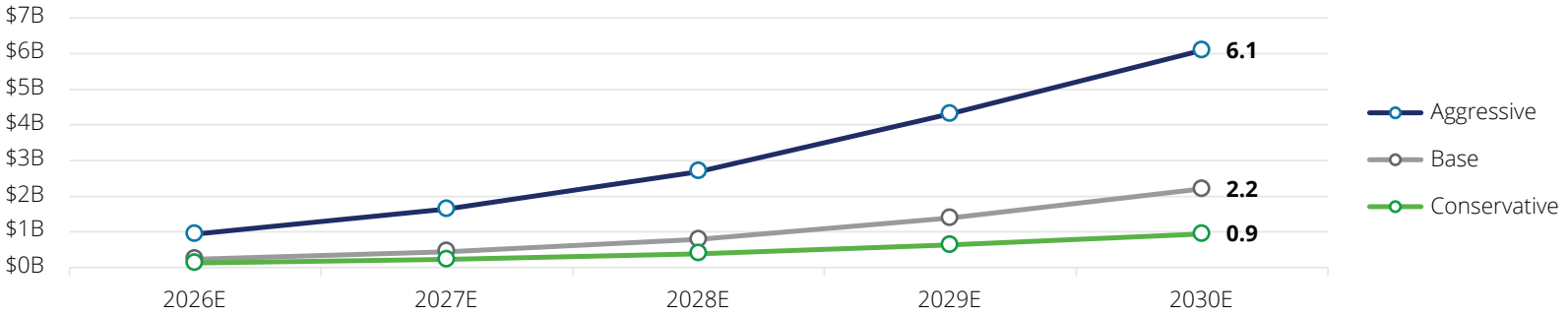
Deloitte.

Fraud in agentic commerce is expected to grow exponentially

Payments fraud by AI agents is fast emerging as a major challenge for financial institutions, payment processors, and e-commerce organizations. The expected growth of agentic commerce may change how fraud happens, how fast it spreads, and the scale of potential losses. Banks and merchants may struggle to tell whether an agent is acting on behalf of a consumer or has been hijacked by fraudsters or their agents. Signals to detect this fraud are still emerging. Responsibility for losses remains unclear.

Deloitte estimates agentic commerce fraud losses could reach more than **$6.1 billion by 2030** in the most aggressive scenario. Banks and payment providers may need to strengthen existing controls and develop new ways to verify agents, detect compromised activity, and establish who bears the loss.

Potential growth in agentic commerce fraud, 2026E–2030E



Agentic commerce fraud could reach
$6.1 billion in 2030

Sources: Deloitte analysis; BILL Holdings FY2026 10-K; The Nilson Report; Federal Reserve Bank of Kansas City.

Key assumptions

US retail e-commerce is expected to grow from $1.23 trillion in 2025 to $1.73 trillion in 2030, at an annual growth rate of 7%.[1]

Agentic commerce fraud is based on two other assumptions: agent-executed share of e-commerce in 2030, and the blended fraud rate (basis points, bps) across 10 fraud types.

Agent-executed share of e-commerce, 2030E



Blended fraud rate, 2030E



Source: 1. Deloitte Center for Financial Services analysis of US department of commerce data

10 fraud types driving agentic commerce fraud

Seven of these fraud types already exist in e-commerce today; AI agents just magnify them. The other three are new because of agents.

New fraud types — Because of AI agents

Agent impersonation — Fake agent claims authority that was never granted.
Prompt/tool manipulation — Malicious content redirects the agent.
Agent error — Exceeds delegated authority or intent, no adversary needed.

Existing fraud types in e-commerce today

Account takeover (ATO) — Compromised account or agent token; credential theft.
Synthetic identity — Fabricated identity opens a new account.
Card-not-present (CNP) — Stolen payment credential in remote checkout.
Authorized push payment (APP) — Push transfer via social engineering.
Transaction laundering — Automated pass-through and mule accounts.
Refund/promotion abuse — Automated exploitation of refund or return rules.
Friendly fraud — Dispute of a legitimate agent purchase; chargeback abuse.

Six starting considerations to mitigate agentic commerce fraud

1. Bind agent identity to a verified human
Consider signed limits at setup, such as amount, merchant, category, time window, not just a valid credential. This is already being built into how agentic payments work industry-wide; enforce it at authorization, not just when the agent is first set up.

2. Authenticate continuously
Don't stop checking at login. A stolen token can carry valid authentication into an unauthorized purchase long after the real session began; verify identity across customer, device, and agent throughout, not just at the start.

3. Add pre-settlement checks
Add confirmation-of-payee and step-up checks before instant settlement. Real-time rails removed the recovery window banks used to catch and reverse fraud; don't rely on a safety net that no longer exists.

4. Define liability rules in advance
Decide now who bears the loss when an agent overreaches, consumer, merchant, or bank. Existing rules cover ATO and CNP; agent impersonation and prompt manipulation have none yet. Don't let the first big dispute set the precedent.

5. Set clear consumer expectations
Tell customers what's covered if an agent overspends or gets manipulated, the same way issuers already explain chargeback rights. Don't leave them to find out for the first time during a dispute.

6. Adopt shared agent-identity standards
Don't build proprietary verification alone. Shared industry protocols for agentic payments are already emerging and gaining real adoption. Join what's forming rather than compete with it.

Agentic commerce fraud is evolving rapidly. Let's talk.



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



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

Disclaimer
For general informational purposes only; not financial, legal, or professional advice. Forecasts are modeled estimates from stated assumptions, not guarantees of future results, and should not be relied on without independent verification.

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.

Copyright © 2026 Deloitte Development LLC. All rights reserved.