

Philosophical Meanderings  
Peripherally Related To  
Artificial Intelligence Research

Win the "most original  
Paper Title" award  
for 1984

by

Alex Lewis and Jeb Beckwith

Artificial Intelligence

Professor Hirshfield

May 11, 1984

Very well done, guys

|         |   |
|---------|---|
| content | A |
| style   | A |
| overall | A |

The author's first paper on artificial intelligence, May 11, 1984.

# Who Is Behind the Agent at Your Window?

HSBC paid \$1.92B for not knowing its customers. The next bill comes for not knowing the people behind their agents.

John Beckwith | Cooper Beckwith, LLC

October 4, 2026 | Public sources current through October 3, 2026

On December 11, 2012, HSBC Holdings and HSBC Bank USA admitted to anti-money laundering and sanctions violations, agreed to forfeit \$1.256B under a five-year deferred prosecution agreement, and accepted an independent monitor. On top of the forfeiture came \$665MM in civil penalties, \$500MM to the OCC and \$165MM to the Federal Reserve. The total was \$1.92B, which the Department of Justice called "the largest penalty in any BSA prosecution to date."<sup>1</sup>

The facts behind the number are the lesson. At least \$881MM in drug trafficking proceeds, including money from the Sinaloa Cartel in Mexico and the Norte del Valle Cartel in Colombia, moved through HSBC Bank USA. From 2006 to 2009 the bank failed to monitor more than \$670B in wire transfers and more than \$9.4B in purchases of physical U.S. dollars from its own Mexican affiliate, HSBC Mexico. Through those same years HSBC Bank USA rated Mexico as "standard" risk, its lowest category.<sup>1</sup> A Senate investigation published that summer traced how a U.S. affiliate became the dollar gateway for a foreign affiliate whose customers the U.S. bank never knew.<sup>2</sup>

Read the structure, not the headline. The money did not arrive from strangers at a branch. It arrived through an intermediary the bank trusted by default, carrying customers the bank never identified. HSBC knew its counterparty. It did not know the principals behind the counterparty's traffic. That is the gap an AI agent opens at your institution, and the subject of this paper.

## Executive Summary

An AI agent can now open a session at your institution with your customer's credentials, read the account and move money, and to your systems it looks like the customer. In sixteen months the card networks, Google, Ant International and a Singapore regulator's platform have built a layer they call Know Your Agent to identify those agents, while the federal banking agencies have placed agentic AI outside the scope of their model risk guidance and the CFPB's open banking rule sits enjoined.<sup>3,4,5</sup> The gap is the one HSBC paid \$1.92B for in 2012: knowing the counterparty and not the principals behind its traffic.<sup>1</sup>

This paper makes four points. Know Your Agent sits on top of Know Your Customer and never replaces it, because the agent is never the customer. Four parties stand behind each agent-initiated transaction: the principal, the operator, the agent instance and the developer. An institution has to be able to name the chain. The first expectations will arrive from state examiners, core providers and network rules, in that order, ahead of a federal rule. The practical work is a file, a mandate, a risk rating and a question: who is behind the agent? Section 1 lists ten things to do now. The rest of the paper is the evidence.

## 1. What to Do Now

Each of these fits on one page of a board packet. None requires a new system.

1. **Write the sentence into your account agreement.** The customer is the person who signed. An agent acting for that customer acts under the customer's authority and at the customer's risk, within the limits you set.
2. **Add an agent block to the customer record.** Operator name, product or model name, mandate on file, date of consent, date of last review. Start the Know Your Agent file next to the KYC file.
3. **Require registration before access.** No agent reaches an account until its operator is identified and a signed mandate is on file.
4. **Map the chain for each agent.** Principal, operator, developer. Treat the chain the way you treat beneficial ownership under the CDD rule.<sup>6</sup>

5. **Ask your core provider and your card processor for two dates.** When the agent indicator appears in your transaction data, and when agent registration appears in your onboarding tools.
6. **Decide, in writing, whether you accept agent-initiated transactions at all.** By channel, by product and by limit. A decision not to accept them is still a decision, and it needs a review date.
7. **Train the front line on three questions.** Who is the agent, who does it belong to, and who authorized it.
8. **Put a one-page Know Your Agent risk appetite statement on the board agenda this quarter.** What you accept, what you refuse, and who signs off on exceptions.
9. **Re-verify the principal before delegation.** A delegation to an agent is a new access event, and it deserves the same identity assurance as a new signer.
10. **Keep the KYC program whole.** Know Your Agent stacks on CIP and CDD. Nothing in this paper replaces either.

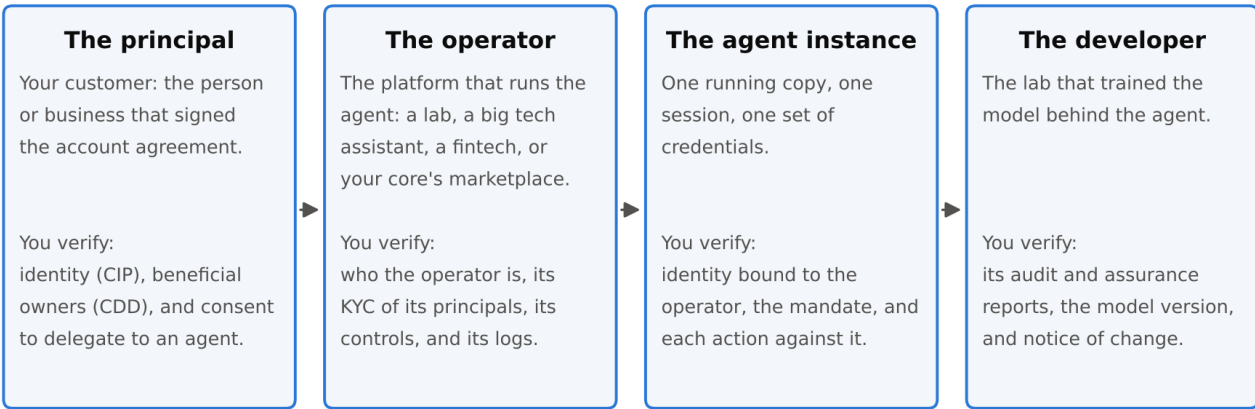
## 2. What an Agent Is, and What It Is Not

The word agent means three things at once, and the confusion costs money. A lawyer hears agency law: a person authorized to act for a principal, with duties running back to that principal. A compliance officer hears the Uniform Electronic Transactions Act, which since 1999 has recognized an "electronic agent" as a tool whose actions bind the person who uses it.<sup>7</sup> A technologist hears software that plans and acts on its own across many steps, with a model from a frontier lab underneath and a platform operating it. All three meanings will be in the room when the first dispute arrives.

The law already answers the first question. A tribunal in British Columbia settled it for a chatbot in February 2024, after Air Canada argued its chatbot was a separate legal entity responsible for its own words. The tribunal rejected the argument: "It makes no difference whether the information comes from a static page or a chatbot."<sup>8</sup> The deployer owns the output. UETA says the same about contracts formed by electronic agents. Responsibility flows to the user of the machine.<sup>7</sup> An agent is never the customer. The customer is the person or business that signed the account agreement, and the agent is that customer's instrument.

That leaves a chain, not a single party, between you and the money (Exhibit 1). The principal is your customer. The operator is the platform that runs the agent: a frontier lab's assistant, a big tech wallet, a fintech, or an agent sold through your core provider's marketplace. The agent instance is the running copy with its own credentials and its own session. The developer is the lab that trained the model. Know Your Customer covers the first link. Know Your Agent covers the chain.

**Exhibit 1. The four parties behind an agent-initiated transaction, and what an institution verifies at each link**



*Know Your Customer covers the first box. Know Your Agent covers the chain.*

Source: the author's framework.

## 3. Why Your KYC Program Cannot See the Agent

The Customer Identification Program rule requires you to form a reasonable belief that you know the true identity of each customer, meaning the person opening the account.<sup>9</sup> The beneficial ownership rule extends that to the people who own or

control a legal entity customer.<sup>6</sup> Both rules identify people at the account opening and on a review cycle. Neither identifies who is moving money through the account on a given afternoon, as long as the mover holds valid credentials.

An agent holds valid credentials. The customer handed them over. From the core system's point of view the agent is the customer, logging in from a new device, moving faster than a person and never sleeping. HSBC's monitoring saw HSBC Mexico, a trusted affiliate with valid access, and did not see the cartel customers behind it. Your monitoring will see a logged-in customer and not the operator behind the session, or the thousands of other principals that operator serves.

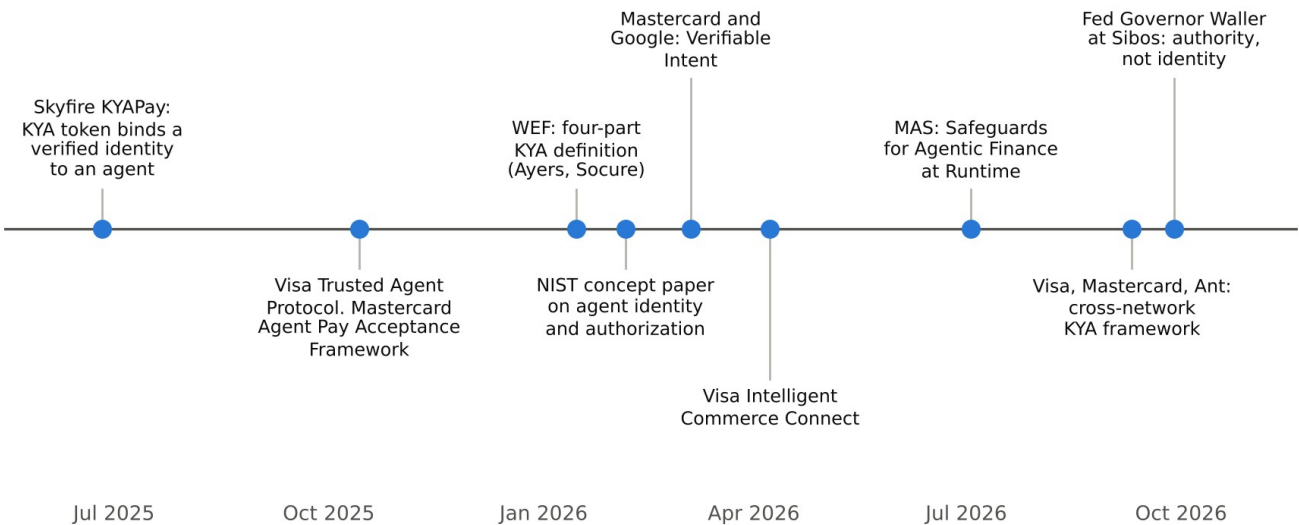
Johnny Ayers, the chief executive of Socure, drew the line in January 2026. Agent identity "is only as trustworthy as the underlying human or organizational identity it represents," and "without high-assurance KYC, even the strongest KYA framework collapses."<sup>10</sup> The same essay gave the four-part definition the industry now uses. Establish who and what the agent is. Confirm what it is permitted to do and for whom. Maintain accountability for each action it takes. Monitor its behavior continuously.<sup>10</sup> David Birch, writing a month later, called agents "unbanked ghosts" and set out the plumbing they lack: identifiers, protected keys, and a standard way to present credentials.<sup>11</sup>

Here is the working definition I use. Know Your Agent is the set of controls by which an institution establishes an agent's identity, the identity of the principal and the operator behind it, the scope of authority delegated to it, and a record of what it did, with monitoring that runs continuously rather than at onboarding. It sits on top of CIP and CDD. It never replaces them.

#### 4. The Industry Is Building This Without You

The timeline in Exhibit 2 runs sixteen months. In June 2025 Skyfire shipped a KYA token that binds a verified human or business identity to an agent, with spending limits inside the token.<sup>12</sup> In October 2025 Visa launched the Trusted Agent Protocol with Cloudflare, so a merchant can tell a signed, registered agent from a hostile bot, and Mastercard published an acceptance framework that registers agents and attaches purchase intent data to each transaction: agent-assisted or autonomous, cart contents, limits and validity windows.<sup>13,14</sup> Google's Agent Payments Protocol had already arrived in September 2025 with more than sixty partners and a cryptographic mandate the user signs so consent can be audited later.<sup>15</sup>

Exhibit 2. Sixteen months of Know Your Agent announcements, June 2025 to September 2026



Sources: company, standards body and regulator documents cited in the endnotes.<sup>12,13,14,10,16,17,18,19,3,20</sup>

In 2026 the pace picked up. Mastercard and Google released Verifiable Intent in March, one record binding identity, intent and action.<sup>17</sup> Visa opened Intelligent Commerce Connect in April to accept agents running on four different protocols.<sup>18</sup> In September, Visa, Mastercard and Ant International announced the first cross-network Know Your Agent framework, convened through the Monetary Authority of Singapore's BuildFin platform, with three pillars: operator traceability across networks, shared certification requirements, and continuous transaction monitoring. The release projects that agents will

orchestrate \$3T to \$5T of global consumer commerce by 2030.<sup>3</sup> Fortune's headline nine days later was blunt. Banks face a new compliance challenge.<sup>21</sup>

Then the Federal Reserve spoke. On September 28, 2026, Governor Christopher Waller told the Sibos conference in Miami: "The question shifts from proving that a buyer is an authorized payer to proving that an agent has the authority to pay on the buyer's behalf." He asked who is on the hook when an agent makes the wrong purchase, warned that fraud systems "calibrated to human behavior, may not translate well to agents," and said the question to watch is whether standards end up platform-specific or interoperable, because interoperable standards "could help to level the playing field for smaller merchants and payment providers."<sup>20</sup>

Notice who is in these announcements and who is not. Card networks, a Chinese payments group, Google, a Singapore regulator's platform. No community bank. No credit union league. No state supervisor. The standards that will decide what an agent has to present at your door are being written by parties whose economics are not yours.

## 5. Who Moves First: The Order of Arrival

---

The federal banking agencies have said, in effect, not yet. The revised model risk guidance of April 2026 replaced SR 11-7, put generative and agentic AI out of scope as "novel and rapidly evolving," aimed its attention at institutions above \$30B in assets, and stated that non-compliance "will not result in supervisory criticism."<sup>4</sup> Vice Chair Bowman explained the thinking in May: supervisors had "expanded the scope of the previous guidance beyond its original purpose," and third-party risk guidance would be simplified next.<sup>22</sup> FinCEN's April proposal to overhaul the AML program rules rewards institutions that use "innovative tools such as artificial intelligence" and says nothing about agents as a typology.<sup>23</sup> The CFPB's open banking rule, the one place a federal rule names the third parties who access accounts on a consumer's behalf, is enjoined and being rewritten with no timeline.<sup>5</sup>

So the first Know Your Agent expectations will reach you from three other directions, in this order.

**State examiners.** On September 16, 2026 the Conference of State Bank Supervisors released an AI Supervisory Framework that covers agentic AI by name, asks for AI inventories, written policies and vendor due diligence, and sorts uses into low, moderate and high risk tiers. State regulators supervise about 79 percent of U.S. banks.<sup>24</sup> For federally insured credit unions, the NCUA's AI resource hub routes AI oversight through the existing third-party guidance rather than through new rules.<sup>25</sup>

**Your core provider.** Fiserv launched agentOS in May 2026 with wide availability targeted for August, running across its core, payments, issuer processing and servicing platforms, co-developed with six banks and credit unions and built on "identity-bound execution, policy enforcement, observability and traceability."<sup>26</sup> When your core ships agents with their own identities, the contract and the configuration screens become your first Know Your Agent policy, whether or not you wrote one.

**Network rules.** Agent registration, intent data and the allocation of losses on card rails arrive through operating rules you accept by default.<sup>14,18</sup>

### If you are between \$20B and \$150B

The \$30B line in the April guidance puts most of this tier inside the primary scope of model risk expectations, even though agentic AI sits outside the guidance itself.<sup>4</sup> Institutions with broker-dealer affiliates answer to FINRA as well. Its 2026 oversight report defines AI agents as "systems or programs that are capable of autonomously performing and completing tasks on behalf of a user" and expects firms to track agent actions, set guardrails and decide where human review is mandatory.<sup>27</sup> Abroad, the Financial Stability Board's June 2026 consultation lists individual identifiers for agents and complete audit trails among twelve sound practices, and the UK's Mills Review calls for "robust frameworks covering data access, identity, authority to act, transaction execution and accountability."<sup>28,29</sup> Examiners read these documents. So should the risk committee.

## 6. What Knowing the Principal Means Now

---

Three things change in practice.

**The record changes.** Beside the CIP file, keep an agent file: the operator's identity, the product or model, the mandate the customer signed, the date of consent, the date of last review, and the revocation path. Treat the chain in Exhibit 1 the way

the CDD rule treats beneficial ownership. You want the natural persons at the end of it, and the entities in between named.<sup>6</sup>

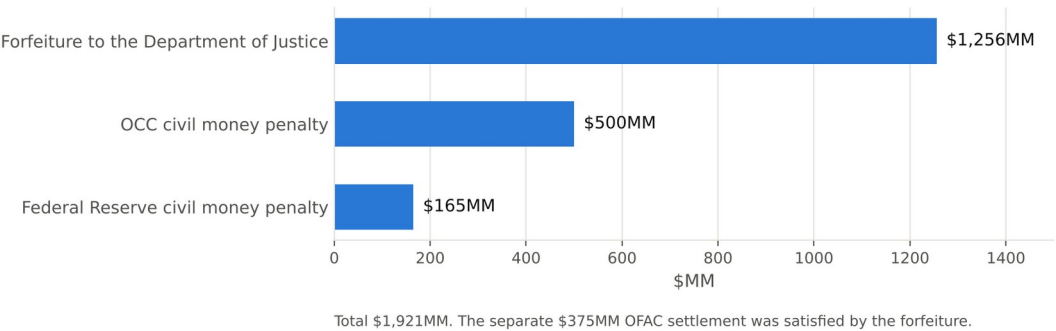
**Consent changes.** A customer who delegates to an agent has created a new access event. The mandate is the new signature card. Mastercard's Verifiable Intent, Google's mandates and Visa's signed headers all exist to make that consent provable to a third party after the fact.<sup>17,15,13</sup> Singapore's regulator went further in July 2026 with a runtime framework in which an agent's identity is resolved against a registry before each action and "an agent cannot expand its own mandate by reasoning inference."<sup>19</sup> For a depository, the mandate belongs in the customer file, not only in the network's records.

**Monitoring changes.** The IMF's April 2026 note on agentic payments warns that agent-mediated actions complicate "the origin and intent behind payments," strain AML monitoring, and create a stability risk when many agents behave alike.<sup>30</sup> Perpetual KYC replaced the periodic review for the same reason. Know Your Agent will be continuous or it will be theater.

**Rate the agent the way you rate the customer.** Your BSA program already assigns a risk rating at onboarding and adjusts it with behavior. An agent deserves the same treatment. Five inputs do most of the work: the operator's identity and track record, the model's provenance and version, the breadth of the mandate, the agent's behavioral history at your institution, and its incident record elsewhere. A read-only agent from a registered operator on a narrow mandate is low risk. An agent with payment authority, a broad mandate and a new operator is high risk, and it gets the controls a high-risk customer gets: lower limits, more frequent review, and a person in the loop above a threshold.

**A worked example.** A small business customer connects an accounts payable agent sold through a well-known platform. The agent reads invoices and pays vendors from the operating account. Under the approach in this paper the file holds the operator's name, the product, a mandate signed by the business owner limiting payments to named vendors under a monthly cap, the consent date and a review date. The transaction record carries the agent indicator. The agent's risk rating is moderate: a registered operator, a bounded mandate, payment authority. When the agent tries to pay a vendor outside the list, the control is not the fraud model guessing. It is the mandate, checked against the payee, that stops the payment and routes it to a person.

**Exhibit 3. What HSBC paid in December 2012 for not knowing the principals behind its affiliate's traffic**



Source: U.S. Department of Justice, December 11, 2012.<sup>1</sup>

None of this requires a new system this year. It requires a decision about what you will accept, a file, and a question you are prepared to ask of your core, your processor and your customer: who is behind the agent?

## 7. Conclusion

HSBC knew its counterparty and not the principals behind it, and the bill was \$1.92B and five years under a monitor. The agent era rebuilds that structure at institution after institution, at machine speed, with the intermediary chosen by the customer rather than by the bank. The federal rulebook is silent for now. The networks, the state supervisors and the core providers are not.

I wrote in September that a number you cannot trace to its source does not belong in your books.<sup>31</sup> The same rule applies to a transaction. If you cannot say who stood behind the agent that moved the money, you did not know your customer. You knew a login.

## Endnotes

---

1. U.S. Department of Justice, "HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit \$1.256 Billion in Deferred Prosecution Agreement," press release, December 11, 2012. <https://www.justice.gov/archives/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations>
2. U.S. Senate Permanent Subcommittee on Investigations, "U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History," hearing and report, July 17, 2012. <https://www.hsgac.senate.gov/subcommittees/investigations/hearings/u-s-vulnerabilities-to-money-laundering-drugs-and-terrorist-financing-hsbc-case-history/>
3. Visa, Mastercard and Ant International, "Visa, Mastercard, and Ant International Build First Cross-Network Know Your Agent Framework," Business Wire release, September 2026. <https://finance.yahoo.com/technology/ai/articles/visa-mastercard-ant-international-build-111358124.html>
4. Office of the Comptroller of the Currency, "Model Risk Management: Revised Guidance," OCC Bulletin 2026-13, April 2026, with analysis by Sullivan & Cromwell LLP, "Federal Banking Agencies Issue Revised Guidance on Model Risk Management," April 17, 2026. <https://www.occ.gov/news-issuances/bulletins/2026/bulletin-2026-13.html>
5. Ballard Spahr LLP, Consumer Finance Monitor, "Open banking regulation in 2026: federal regulation resurfaces as states bring data sharing into focus," June 26, 2026. <https://www.consumerfinancemonitor.com/2026/06/26/open-banking-regulation-in-2026-federal-regulation-resurfaces-as-states-bring-data-sharing-into-focus/>
6. Beneficial ownership requirements for legal entity customers, 31 CFR 1010.230. <https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1010/subpart-B/section-1010.230>
7. Proskauer Rose LLP, "Contract Law in the Age of Agentic AI: Who's Really Clicking 'Accept'?", April 9, 2025. <https://www.proskauer.com/blog/contract-law-in-the-age-of-agentic-ai-whos-really-clicking-accept>
8. Moffatt v. Air Canada, 2024 BCRT 149 (British Columbia Civil Resolution Tribunal, February 14, 2024), as summarized by McCarthy Tétrault, "Moffatt v. Air Canada: misrepresentation by an AI chatbot," 2024. <https://www.mccarthy.ca/en/insights/blogs/techlex/moffatt-v-air-canada-misrepresentation-ai-chatbot>
9. Customer Identification Programs for banks, savings associations, credit unions, and certain non-federally regulated banks, 31 CFR 1020.220. <https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1020/subpart-B/section-1020.220>
10. Johnny Ayers, "AI agents could be worth \$236 billion by 2034. Here's why trust matters," World Economic Forum, January 15, 2026. <https://www.weforum.org/stories/2026/01/ai-agents-trust/>
11. David G.W. Birch, "KYA now," February 19, 2026. <https://dgwbirch.substack.com/p/kya-now>
12. Skyfire, "Skyfire Launches Open KYAPay Protocol With Agent Checkout," Business Wire, June 26, 2025. <https://www.streetinsider.com/Business+Wire/Skyfire+Launches+Open+KYAPay+Protocol+With+Agent+Checkout/24981183.html>
13. Digital Transactions, "Visa Launches Trusted Agent, an Agentic-Commerce Protocol," October 14, 2025. <https://www.digitaltransactions.net/visa-launches-trusted-agent-an-agentic-commerce-protocol/>
14. Mastercard, "Agent Pay Acceptance Framework," October 14, 2025. <https://www.mastercard.com/am/en/news-and-trends/stories/2025/agentic-commerce-framework.html>
15. eco.com, "Agent identity verification: how AI agents authenticate purchases in 2026" (Mastercard Agent Pay, Visa Trusted Agent Protocol, Google Agent Payments Protocol), 2026. <https://eco.com/support/en/articles/15192005-agent-identity-verification-how-ai-agents-authenticate-purchases-in-2026>
16. National Institute of Standards and Technology, "New Concept Paper: Identity and Authority for Software Agents" (NCCoE, "Accelerating the Adoption of Software and AI Agent Identity and Authorization"), February 5, 2026. <https://www.nist.gov/news-events/news/2026/02/new-concept-paper-identity-and-authority-software-agents>
17. Mastercard, "Verifiable Intent," March 5, 2026. <https://www.mastercard.com/global/en/news-and-trends/stories/2026/verifiable-intent.html>
18. Visa, "Visa opens the door to AI-driven shopping for businesses worldwide" (Visa Intelligent Commerce Connect), press release, April 8, 2026. <https://corporate.visa.com/en/sites/visa-perspectives/newsroom/visa-intelligent-commerce-connect-ai-shopping-for-businesses.html>
19. Monetary Authority of Singapore, Information Paper, "Safeguards for Agentic Finance at Runtime" (SAFR), July 3, 2026, as summarized by Ashurst Perkins Coie, "MAS SAFR Explained," July 2026. <https://www.ashurstperkinscoie.com/en/insights/mas-safr-explained-singapores-runtime-governance-standard-for-agentic-ai-in-finance/>
20. Christopher J. Waller, "Payments in the Age of AI Agents," speech at Sibos 2026, Miami, Board of Governors of the Federal Reserve System, September 28, 2026. <https://www.federalreserve.gov/newsevents/speech/waller20260928a.htm>
21. Nicholas Gordon, "'Know your agent': Banks face a new compliance challenge as AI agents shop and pay on their own," Fortune, September 19, 2026. <https://fortune.com/2026/09/19/know-your-agent-ai-payments-banks/>
22. Michelle W. Bowman, "Artificial Intelligence in the Financial System," speech, Board of Governors of the Federal Reserve System, May 1, 2026. <https://www.federalreserve.gov/newsevents/speech/bowman20260501a.htm>
23. Financial Crimes Enforcement Network, Notice of Proposed Rulemaking on anti-money laundering and countering the financing of terrorism programs, April 7, 2026, as reported by Fintech Global, "FinCEN reform puts AI at the heart of AML/CFT compliance," April 23, 2026. <https://fintech.global/2026/04/23/fincen-reform-puts-ai-at-the-heart-of-aml-cft-compliance/>
24. Conference of State Bank Supervisors, Artificial Intelligence Supervisory Framework, September 16, 2026, as summarized by White & Case LLP, "CSBS releases Artificial Intelligence Supervisory Framework," September 2026. <https://www.whitecase.com/insight-alert/csbs-releases-artificial-intelligence-supervisory-framework>
25. Troutman Pepper Locke, Consumer Financial Services Law Monitor, "NCUA Issues Updated AI Resource Hub," January 2026. <https://www.consumerfinancialserviceslawmonitor.com/2026/01/ncua-issues-updated-ai-resource-hub/>
26. Fiserv, "Fiserv Launches agentOS: The Operating System for Agentic AI in Banking," GlobeNewswire, May 14, 2026. <https://www.globenewswire.com/news-release/2026/05/14/3294727/0/en/Fiserv-Launches-agentOS-The-Operating-System-for-Agentic-AI-in-Banking.html>
27. Debevoise & Plimpton LLP, "FINRA's 2026 Regulatory Oversight Report: Continued Focus on Generative AI and Emerging Agent-Based Risks," December 2025. <https://www.debevoise.com/insights/publications/2025/12/finras-2026-regulatory-oversight-report-continued>

28. Financial Stability Board, "Sound Practices for Responsible Adoption of Artificial Intelligence (AI)," consultation report, June 10, 2026, with summary by TechInformed, "FSB calls for tighter controls on agentic AI in finance," June 2026. <https://www.fsb.org/2026/06/fsb-consults-on-sound-practices-for-the-responsible-adoption-of-artificial-intelligence-ai/>
29. Norton Rose Fulbright, Regulation Tomorrow, "FCA publishes Mills Review into AI and the future of retail financial services," July 2026. <https://www.regulationtomorrow.com/2026/07/fca-publishes-mills-review-into-ai-and-the-future-of-retail-financial-services/>
30. Sonja Davidovic and Hervé Tourpe, "How Agentic AI Will Reshape Payments," IMF Notes 2026/004, International Monetary Fund, April 2026. <https://www.imf.org/en/publications/imf-notes/issues/2026/04/22/how-agentic-ai-will-reshape-payments-575560>
31. John Beckwith, "AI Risk in Depositories: The Need for Elicitability," AI Risk in Finance (Substack), September 17, 2026. <https://jebbeckwith.substack.com/p/ai-risk-in-depositories-the-need>