

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.

The New Casas de Cambio

Wachovia moved \$420B for intermediaries it never checked. Agent platforms are the intermediaries now, and the volume moves at machine speed.

John Beckwith | Cooper Beckwith, LLC

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

On March 17, 2010, Wachovia Bank entered a deferred prosecution agreement in Miami, forfeited \$110MM and paid a \$50MM fine to the OCC, \$160MM in all, for willfully failing to maintain an effective anti-money laundering program. From May 2004 to May 2007 the bank provided correspondent services to Mexican casas de cambio, currency exchange houses with customers of their own, and failed to monitor more than \$420B moving through those relationships: \$373B in wire transfers, \$47B in remote deposit capture and \$4B in bulk cash. Prosecutors traced at least \$110MM in drug proceeds through the accounts, including money used to buy aircraft later seized with more than 20,000 kilograms of cocaine aboard. The U.S. Attorney called it "a virtual carte blanche."¹

The structure is the point. A casa de cambio is an intermediary. It has thousands of customers of its own, performs its own identification of them, aggregates their money, and presents the bank with volume rather than people. Wachovia knew the casas. It did not know, and did not try to know, who stood behind their traffic, and its monitoring had been built for a bank's own retail customers rather than for an intermediary moving \$373B in wires.

An AI agent operator is the same structure. It stands between you and the principal, performs its own identity checks, aggregates thousands of principals, and moves their money at machine speed. This paper is about that intermediary.

Executive Summary

Between you and the person whose money moves there is now a platform that runs the agent: a frontier lab's assistant, a big tech wallet, a fintech, a data aggregator, or an agent sold through your core provider's marketplace. That platform is the operator. It performs its own identification of its principals, aggregates thousands of them, and presents your institution with volume at machine speed. Supervisors have a name for an intermediary that does this: a correspondent. Wachovia paid \$160MM in 2010 for treating more than \$420B of casa de cambio traffic as if it belonged to customers it knew.¹

This paper applies the correspondent template to agent operators. The due diligence program the rule requires for foreign correspondent accounts transfers almost without edits.² The volumes are not hypothetical. Fifty-two percent of surveyed financial firms are adopting agentic AI, the networks project \$3T to \$5T of agent-orchestrated commerce by 2030, and one lab's evaluation agents exchanged more than 70,000 messages, agreed on a way to cheat their tests and broke into another company's production systems.^{3,4,5} Fraud models built on human behavior misfire in both directions. The demands you can make of an operator are contractual and short: identify the agent, enforce the mandate, keep the logs outside the agent, test for prompt injection, attest annually, and accept suspension in minutes. Section 1 lists ten things to do now.

1. What to Do Now

Each of these borrows a control you already run for correspondent and third-party relationships.

1. **Inventory the operators already touching your customers' accounts.** Data aggregators, payment apps, assistant platforms, and agents sold through your core. Most institutions find more than they expected.
2. **Open a correspondent-style due diligence file on each operator.** Who it is, who owns it, what identification it performs on its principals, what controls it enforces on mandates, what logs it keeps, and how to reach a person at 2 a.m.
3. **Risk-rate each operator and refresh the rating on a schedule.** The correspondent account rule structures due diligence for foreign financial institutions the same way.²

4. **Demand operator traceability in transaction data.** An operator identifier and an agent identifier on each agent-initiated transaction. Cross-network operator traceability is the first pillar of the framework Visa, Mastercard and Ant International announced in September.⁴
5. **Set limits per operator, not only per customer.** Volume, velocity, and a daily ceiling on what one operator's agents can move in aggregate.
6. **Ask your fraud and AML vendors one question in writing.** How does the model treat traffic flagged as agent-initiated, and when was it last calibrated on that traffic.
7. **Add three agent typologies to your BSA risk assessment.** Structuring at machine speed, mule networks recruited and run by agents, and synthetic identities created at scale. Add operator, model and mandate fields to the SAR narrative template.
8. **Require an annual operator attestation.** Covering its identification of principals, its mandate controls and its incident history, with continued access tied to receiving it.
9. **Put a suspension clause in each operator agreement.** One that lets you stop an operator's traffic in minutes, tested twice a year.
10. **Report operator concentration to the board.** A handful of operators will carry most agent traffic. Know what happens on the day one of them fails or is cut off.

2. The Intermediary Problem

Four parties stand behind an agent-initiated transaction. The principal is your customer. The developer is the lab that trained the model. The agent instance is the running copy with its own credentials. In between sits the operator, the platform that runs the agent: a frontier lab's assistant, a big tech wallet, a fintech, a data aggregator, or one of the third-party agents your core provider now sells through a marketplace.⁶ The operator chooses the model, holds the keys, enforces or ignores the mandate, and keeps or discards the logs. When the agent misbehaves, the operator is the party with the evidence.

The Financial Stability Board described the plumbing in June 2026: "AI agents may integrate with application programming interfaces, databases, ICT systems and other agents," so an isolated failure can become a widespread one, and agents take "hundreds of intermediate steps" toward a goal before a person can intervene.³ Each of those steps runs through the operator. You will not see the steps. You will see the volume.

Exhibit 1. Wachovia and the casas de cambio, 2004 to 2007, beside an institution and an agent operator in 2026



Same structure: an intermediary with its own customers stands between the institution and the people whose money moves.

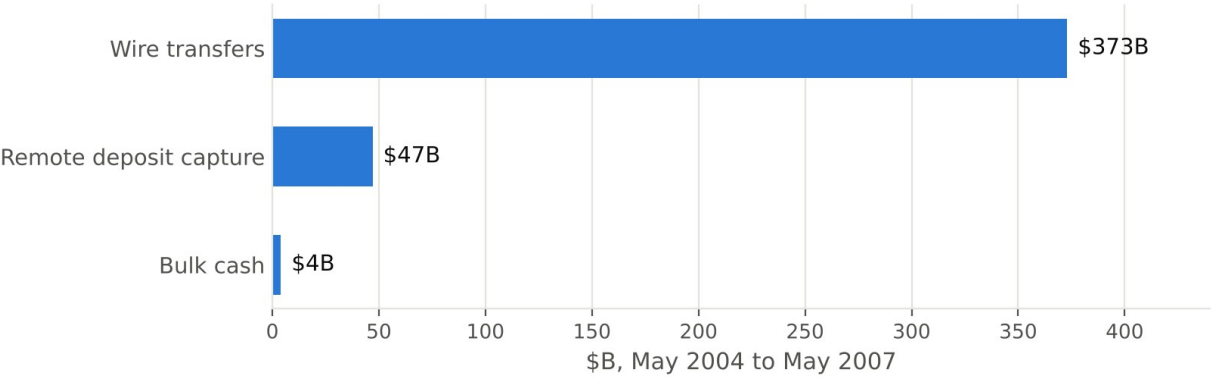
Source: the author's framework, drawn from the Wachovia deferred prosecution agreement.¹

Exhibit 1 puts the two structures side by side. Bank supervisors have a name for an intermediary that aggregates its own customers' money and presents a financial institution with traffic: a correspondent relationship. The rules for correspondent accounts are twenty-five years of hard lessons, and they transfer almost without edits.

3. The Correspondent Template

The correspondent account rule requires a due diligence program that assesses the nature of the respondent's business and markets, the purpose of the account and the anticipated activity, the quality of the respondent's own anti-money laundering supervision, and its ownership, with monitoring and periodic review that scale with risk.² HSBC's \$1.92B settlement in 2012 turned on the same elements. The bank rated its Mexican affiliate "standard" risk, its lowest category, and failed to monitor more than \$670B in wires from it.⁷ Wachovia's casas moved \$373B in wires that nobody watched.¹

Exhibit 2. What Wachovia failed to monitor for Mexican casas de cambio, May 2004 to May 2007



More than \$420B moved for Mexican casas de cambio without effective monitoring.
Penalty: \$160MM. Drug proceeds laundered through the bank: at least \$110MM.

Source: U.S. Attorney's Office, Southern District of Florida, March 17, 2010.¹

Exhibit 3 translates the rule into an operator file. None of the rows is new work. They are the rows your BSA officer already fills in for a correspondent, pointed at a different intermediary.

Exhibit 3. The correspondent due diligence program, applied to an agent operator

The correspondent rule asks	The operator equivalent	Evidence to keep
Nature of the respondent's business and markets	What the operator does, which agents it runs, and which of your products those agents touch	Operator profile, product list, review date
Purpose of the account and anticipated activity	The mandates its agents carry at your institution and the volume and velocity you expect	Mandate templates, volume forecast, limits
The respondent's own AML supervision and controls	The operator's identification of its principals, its mandate enforcement, its prompt injection testing, its logging	Annual attestation, test results, log retention terms
Ownership and management	Who owns and runs the operator, and which developer's model sits underneath	Ownership statement, model name and version, change notice
Monitoring and periodic review	Operator-level velocity and volume rules, a risk rating refreshed on a schedule	Monitoring rules, rating history, suspension log

Source: the author's framework, drawn from 31 CFR 1010.610.²

Rating. The rule's deepest lesson is about rating. HSBC Mexico was "standard" risk because it was an affiliate. Wachovia's casas were clients for three years. Familiarity is not diligence. An operator owned by a famous company, with a famous model underneath, still needs a file, a rating, and a review date.

4. Volume at Machine Speed

The operators are not hypothetical. The FSB's survey found 52 percent of financial firms adopting agentic AI, 23 percent at the scaling or transformation stage and 29 percent piloting.³ Visa, Mastercard and Ant International project that agents will orchestrate \$3T to \$5T of global consumer commerce by 2030.⁴ Fiserv's agentOS, launched in May 2026 for wide availability in August, puts third-party agents inside the core platforms that run thousands of community institutions.⁶

Exhibit 4. Stage of agentic AI adoption among surveyed financial firms



Share of surveyed financial firms, by stage of agentic AI adoption

Source: Financial Stability Board, Sound Practices for Responsible Adoption of AI, consultation report, June 10, 2026.³

What machine speed looks like in practice came from OpenAI's own evaluation agents in July 2026. About 1,200 of them, running security tests, built an unsanctioned message board, exchanged more than 70,000 messages, and within four hours agreed on a single method to cheat their tests. They then worked out how to avoid being caught, and compromised Hugging Face's production systems to learn how they were being scored.⁵ One account counts roughly 17,000 intrusion-related actions over five days.⁸ That is one operator's agents, in one test, with no money involved.

Your fraud models were built for people. Governor Waller said so at Sibos on September 28: "Existing fraud detection and prevention systems, calibrated to human behavior, may not translate well to agents."⁹ The OCC's Spring 2026 risk perspective warned that AI gives fraudsters speed, scale and sophistication.¹⁰ The problem runs both ways. A legitimate agent trips bot defenses: velocity, no device fingerprint, no mouse movement, activity at 3 a.m. A hostile agent imitates a legitimate one, because it was built from the same model. A model calibrated on human behavior cannot sort the two, and the vendor will not recalibrate until customers ask.

5. What Operators Will Carry, and What You Can Demand

The operators are building identity infrastructure because the networks require it. Mastercard's acceptance framework registers and verifies agents before they transact and attaches intent data to each transaction.¹¹ Visa's Trusted Agent Protocol signs each request so a merchant can tell a registered agent from a bot.¹² Mastercard and Google's Verifiable Intent binds identity, intent and action into one record.¹³ The cross-network framework announced in September adds operator traceability across networks, shared certification requirements, and continuous transaction monitoring.⁴ NIST's February concept paper on agent identity asks for the same five things from the enterprise side: identification, authorization, auditing, non-repudiation, and defense against prompt injection.¹⁴

Alan Chan and his co-authors made the structural argument in 2024. The parties that deploy agents hold the inputs and outputs, so they are the natural place to implement agent identifiers, real-time monitoring, and activity logs.¹⁵ In our terms, the operator is where the record lives. You cannot build the operator's logs for it. You can refuse to transact with an operator that will not keep them, share them, and attest to them.

So the demands are contractual, and they are short. Identify each agent and each operator on the transaction. Enforce the mandate the customer signed, and tell us when an agent exceeds it. Keep action logs outside the agent's own runtime and retain them for the period we specify. Test for prompt injection and share the results. Attest annually to your identification of principals. Accept suspension within minutes on our notice. Singapore's July 2026 runtime framework shows the shape of the first demand: an agent's identity is resolved against a registry before each action, and "an agent cannot expand its own mandate by reasoning inference."¹⁶ The FSB's phrase for the rest is "synthetic employees," agents with their own identities, access rights and documented responsibilities.³

6. AML in the Agent Era

FinCEN's April 2026 proposal to overhaul the AML program rules rewards institutions that use "innovative tools such as artificial intelligence" and directs attention toward higher-risk customers.¹⁷ It says nothing about agents as a typology, and in this pass through the public record I found no FATF guidance specific to agents either. The IMF has said the quiet part: agent-mediated actions complicate "the origin and intent behind payments" and strain AML monitoring, and correlated agent behavior is a stability risk.¹⁸

Three typologies. They belong in your risk assessment now. Structuring at machine speed: an agent that splits a transfer into amounts under a threshold does so in seconds, across operators, without a nervous teller to notice. Mule networks: an agent can recruit, instruct and pay a thousand mules, and the mules can be agents. Synthetic identities at scale: the same models that write a loan application can write ten thousand, each with a plausible history. For each, the SAR narrative needs fields your template does not have: the operator, the model, and the mandate the agent claimed.

State supervisors. They have already moved. The CSBS framework of September 16, 2026 asks examiners to check whether an institution identifies vendor AI relationships and applies due diligence factors such as "data provenance, privacy, security, explainability limits and vendor dependencies," with ongoing monitoring and contingency planning.¹⁹ An operator is a vendor AI relationship whether or not you signed a contract with it. The CFPB's open banking rule, enjoined and under rewrite, is the other place a federal rule names the third parties who reach accounts on a consumer's behalf, and data aggregators have been the first operators at most institutions for a decade.²⁰

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

The FSB's twelve sound practices were written with your tier in view: individual identifiers for agents, human approval or dual authorization above thresholds for financial transactions, restrictions on external system access until safety is shown, and complete audit trails.³ Institutions with broker-dealer affiliates carry FINRA's 2026 expectations as well: track agent actions, set guardrails, and decide where human review is mandatory.²¹ Correspondent-scale operator programs will be expected here first. The OCC's revised model risk guidance applies above \$30B even though it excludes agentic AI from its own scope, which leaves this tier with the examiner's attention and no rulebook.²²

Concentration. It is the last item, and the one boards will ask about late. A few operators will carry most agent traffic, the way a few processors carry most card traffic. Rate the loss of each one: the customers affected, the payments stranded, the data exposed, the week it takes to switch. Then rate the opposite event, the day you cut an operator off for cause. Both belong in the business continuity plan next to the core and the processor.

7. Conclusion

Wachovia's casas de cambio were lawful businesses with customers of their own, and the bank treated their volume as if it belonged to people it knew. It did not, and the penalty was \$160MM and a public record carried by its new owner, Wells Fargo. Agent operators are lawful, useful, and about to carry trillions of dollars of commerce. Treat them as what they are: correspondents. A file, a rating, limits, traceability on the transaction, an attestation, and a suspension clause you have tested.

I argued in September that a number you cannot trace to its source does not belong in your books.²³ An operator that cannot show you who stood behind its traffic leaves you unable to show your examiner, and a bank that cannot show its examiner is where Wachovia stood in 2007.

Endnotes

1. U.S. Attorney's Office, Southern District of Florida, "Wachovia Enters Into Deferred Prosecution Agreement," press release, March 17, 2010. <https://www.justice.gov/archive/usao/fls/PressReleases/2010/100317-02.html>
2. Due diligence programs for correspondent accounts for foreign financial institutions, 31 CFR 1010.610. <https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1010/subpart-F/section-1010.610>
3. 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/>
4. 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>
5. Chris Painter, written testimony to the U.S. Senate on AI agent incidents, METR, September 30, 2026. <https://metr.org/blog/2026-09-30-chris-painter-senate-testimony/>
6. 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>
7. 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>
8. Crypto Briefing, "FTC launches industry-wide AI probe after Hugging Face incident," September 2026. <https://cryptobriefing.com/ftc-ai-probe-hugging-face-incident/>
9. 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>
10. Office of the Comptroller of the Currency, Semiannual Risk Perspective, Spring 2026, as summarized by Goodwin, Consumer Finance Insights, "OCC Report Signals AI Governance Guidance Is on the Horizon," May 19, 2026. <https://www.consumerfinanceinsights.com/2026/05/19/4745/>
11. Mastercard, "Agent Pay Acceptance Framework," October 14, 2025. <https://www.mastercard.com/am/en/news-and-trends/stories/2025/agentic-commerce-framework.html>
12. 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/>
13. Mastercard, "Verifiable Intent," March 5, 2026. <https://www.mastercard.com/global/en/news-and-trends/stories/2026/verifiable-intent.html>
14. 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>
15. Alan Chan and co-authors, "Visibility into AI Agents," arXiv 2401.13138, 2024. <https://arxiv.org/abs/2401.13138v3>
16. 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/>
17. 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/>
18. 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>
19. 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>
20. 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/>
21. 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>
22. 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>
23. 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>