Wells Fargo Ships Section 15 on November 24: Every AI Agent Instruction Is Deemed Authorized by You

On October 3, 2026, Wells Fargo posted a revised Online Access Agreement. Buried in it is Section 15: when an AI agent moves your money, you moved it, with zero further verification required.

Wells Fargo's Section 15 takes effect November 24, 2026. It deems any instruction or transaction submitted by a third-party AI agent to be initiated and authorized directly by the customer, with no further verification, and states that agent use is "AT YOUR OWN RISK." JPMorgan Chase, Citi and Bank of America went the other way in mid-October 2026 and blocked credential-based agents outright.

Four large U.S. banks looked at the same problem in October 2026: AI agents logging into consumer accounts with the customer's own username and password, because that is the only way most of them can get in. Three said no. Wells Fargo wrote a clause instead.

Section 15 deems an agent's instruction to be yours

The new section is titled "Third-Party Artificial Intelligence Agents or Agentic AI" and it triggers if you "use, allow, enable, or authorize the deployment or use of any" AI agent against any Service or Eligible Account. The definition of an AI Agent in the upcoming agreement is wide: "any software, application, program, or other technology that takes autonomous, semi-autonomous, or non-autonomous action on behalf of any person or entity."

Read that definition slowly. "Non-autonomous action on behalf of any person" describes software in general, not agentic AI. A browser extension that fills a form, a password manager that logs you in, a scheduled script that pulls a statement: all of those take non-autonomous action on your behalf. Whether Wells Fargo intends to apply it that broadly is a separate question, and I have no evidence they do. The text does not limit itself to LLM-driven agents.

Three operative pieces follow from the definition:

- Instructions and transactions from an agent are deemed initiated and authorized directly by the customer, without further verification, and Wells Fargo may rely on them as valid and binding.
- "Your use of any AI Agent is AT YOUR OWN RISK." That is the agreement's own capitalization.
- "We do not monitor, review, audit, or certify the security, privacy policies, or data handling practices of any AI Agent or the third party providing such AI Agent."

One more piece gets less attention: Wells Fargo reserves the right to restrict, suspend, terminate or limit access by particular agents. Permission is revocable at the bank's discretion. So the deal is not that agents are allowed. Agents are tolerated, at your risk, until the bank decides otherwise.

The agreement was posted October 3 and the upcoming-agreement page was updated October 26, per Wells Fargo's own banking updates page. Effective date: November 24, 2026.

Three banks said no, one wrote a disclaimer

Jamie Dimon raised agent-in-account risk on JPMorgan's October 13, 2026 earnings call. CNBC reported that Chase blocks outside agents from directly accessing accounts, and a JPMorgan spokeswoman put the reasoning in one sentence: "Because it is not safe, we do not permit third parties to access accounts by obtaining customers' banking credentials and logging in on their behalf."

Citi's position, reported October 23: "We do not permit third-party AI agents or assistants to log into a customer's account or transact directly within our digital banking platforms." Citi allows read-only access through Citi-approved open-banking providers. Bank of America was reported between October 13 and 16 as restricting third-party agents from consumer deposit accounts, and coverage of the wider move notes Charles Schwab and Morgan Stanley responded as well.

BANK	AGENT LOGIN TO ACCOUNT	READ-ONLY VIA OPEN BANKING	AGENT-INITIATED PAYMENTS
Wells Fargo (from Nov 24, 2026)	Permitted, deemed authorized by you, at your own risk	Not specified in Section 15	Treated as your instruction, no further verification
JPMorgan Chase	Blocked	Allowed via providers such as Plaid	Not available on that route
Citi	Blocked	Allowed via Citi-approved providers	Blocked
Bank of America	Restricted from consumer deposit accounts	Not specified in reporting	Not specified in reporting

Chase still supports customer-authorized data sharing through open-banking providers such as Plaid, but that route is limited read-only data. It cannot send money or pay a bill. That constraint is the whole story: the agents people actually want (pay this, move that, cancel the other) need write access, and the only write path available to them today is the login box.

As for a regulated alternative, there is not one right now. The CFPB finalized the Section

1033 personal financial data rights rule in October 2024, with compliance for the largest institutions set for April 1, 2026. A federal court in the Eastern District of Kentucky enjoined enforcement, and the CFPB opened reconsideration in August 2025. The regulated permissioned-access route stalled, so banks are writing the rules themselves through terms of service.

Nobody has tested who eats the loss when an agent gets it wrong

Section 15 is a contractual allocation. It says the bank may treat agent instructions as yours and does not have to verify further. The gap between "the agreement says you authorized it" and "a regulator or a court agrees you authorized it" is where every real dispute will land, and I am not aware of any ruling that settles it.

> ! **The catch in the definition**
> Section 15 applies if you "use, allow, enable, or authorize" an agent, and the definition covers non-autonomous software acting on your behalf. My read: the "allow" and "enable" verbs do real work here. A business customer whose employee connects an agent to a shared account has arguably allowed it, whether or not the account owner knew.

Credential sharing broke Amazon's patience too

The same pattern showed up outside finance in September 2026, when Amazon blocked Meta's Muse shopping agent, citing unauthorized access and credential capture. Different industry, identical mechanics: an agent that needs to act on a user's behalf, a platform with no delegated-authority path for that action, and an agent vendor that solves it by taking the user's password.

Credential sharing breaks the properties you want from an authorization system. The bank cannot tell an agent's session from the customer's. It cannot scope what the agent may do, cannot set a spending limit per agent, cannot revoke one agent without a password reset that kills all of them, and cannot produce an audit trail that distinguishes the human from the software. Session logs show one actor: the customer.

That is why JPMorgan's phrasing is precise. "Because it is not safe" is a statement about what credential-based access makes impossible.

The alternative architecture is well understood. Scoped, revocable, per-agent credentials with least privilege by default. I wrote about Cloudflare's internal AI workspace, where agents start with zero access and gain only task-specific permissions, as one implementation of that idea. The distance between that model and "the agent has the customer's password" is large. The ecosystem shipping these agents also has a weak record here: in my analysis of the Model Context Protocol, 91.8% of public MCP servers shipped without authentication at all.

WHERE I LAND

My take: most coverage framed this as Wells Fargo being open to AI agents while the others are closed. I read it the other way. Blocking is a security decision that costs the bank something: angry customers, a product gap, pressure from fintech partners. Section 15 costs Wells Fargo nothing and transfers the downside to the account holder while keeping an unlimited right to cut agents off anyway. ***The permissive-looking clause is the more defensive move of the two.*** *Chase gave up revenue to avoid the risk; Wells Fargo kept the optionality and priced the risk at zero for itself.*

What to settle before November 24

For anyone building or deploying agents that touch financial accounts, four things are worth deciding now.

Inventory every credential your agents hold, and not just banking ones. Any stored username and password that software uses to act as a user is the same failure mode Amazon cited against Meta's Muse in September 2026. If you cannot name the accounts, you cannot assess the exposure.

Separate read from write and treat them differently. Read-only aggregation through an approved open-banking provider is the route Citi and Chase explicitly still allow. Payment initiation is the route all three block. If your roadmap assumes agent-initiated payments at consumer banks, that assumption has no supported path at three of the four largest

institutions.

Read the clause against your own customers. Section 15 binds the Wells Fargo accountholder. If your product causes a customer to “use, allow, enable, or authorize” an agent against their account, you have made them the party holding the risk. Decide whether you disclose that, indemnify against it, or do not ship the feature.

Assume access is revocable. Wells Fargo reserves the right to restrict, suspend, terminate or limit particular agents, so any individual bank integration can be switched off. Your product has to degrade rather than break.

For an individual customer, the decision is narrower. If you give an agent your Wells Fargo credentials after November 24, the agreement’s position is that whatever that agent does is your instruction and the bank owes you no verification step. Whether that holds up in a real dispute is unsettled, and I would not want to be the test case.

I expect deemed-authorization clauses to spread by mid-2027

I expect the Section 15 language, or something close to it, to show up elsewhere. It is cheap to write, it requires no engineering, and it lets a bank say yes to agentic AI in marketing while holding none of the downside. If it survives its first serious consumer dispute without regulatory pushback, I would expect most of the clause’s structure (deemed authorization, no monitoring duty, revocable access) to appear in other institutions’ terms within two or three update cycles.

I also expect the first high-profile loss to decide this, well before any rulemaking does. A customer loses a meaningful sum to a compromised or confused agent, the bank points at Section 15, and the dispute produces the first public answer on whether a terms-of-service deeming clause can convert an unauthorized transfer into an authorized one. The Section 1033 timeline gives no reason to expect a regulated API path in the same window: finalized October 2024, April 1, 2026 compliance date enjoined, reconsideration open since August 2025.

The thing I am genuinely unsure about is whether the banks blocking agents can hold the

line. Customer demand for agentic banking is real, the blocking position creates a product gap, and the pressure will be commercial rather than technical. If one large institution ships proper scoped delegated authority (per-agent credentials, spending limits, independent revocation, distinguishable audit trails), the rest follow and Section 15 becomes a footnote about the interim period. If nobody ships it, deemed-authorization clauses become the standard, and the risk of a new and poorly understood software category sits with retail customers who clicked through an agreement update.

WHAT TO DO WITH THIS

Section 15 takes effect November 24, 2026, and its practical content is that Wells Fargo will treat an AI agent's instruction as yours without further verification while auditing nothing about that agent. If your product, your treasury process, or your personal accounts depend on software logging in with stored credentials, that exposure is now written into a contract you are party to. If you want a second opinion on where your agent architecture sits against this, Book a call →

WRITTEN BY

Artur Markus

Software engineer in Basel building AI infrastructure and agentic systems, with a background in pharmaceutical automation, GxP compliance, and validation. I help teams turn AI from a chatbot into a reliable operational layer.

Book a meeting →