AffixIO Technical Paper · WP-023
June 2026
affix-io.com

AFFIXIO WHITE PAPER · WP-023

AML, KYC, and Agentic Payments: Compliance for the Machine-to-Machine Economy

When AI agents make payments at machine speed, who is the customer? And how do you prove authorisation without slowing everything down?

AffixIO | United Kingdom | affix-io.com | June 2026

ABSTRACT

Agentic payments, transactions initiated by software acting on a human's behalf, automatically, at scale, are no longer a future concern. They are happening now, across open banking rails, API payment platforms, cryptocurrency networks, and corporate treasury systems. The compliance frameworks that govern these payments were designed with humans in mind: a person walks in, presents identification, gets verified, makes a payment. None of that maps cleanly onto an AI agent that fires two hundred transactions before breakfast. This paper explains the AML and KYC gap that agentic

> payments create, and shows how AffixIO's API provides the proof-based authorisation layer that keeps compliance intact at machine speed.

CONTENTS

SECTION 1

The Rise of the Paying Agent

A few years ago, the idea of software making financial decisions autonomously felt like a science-fiction scenario. Today it is a business requirement. Companies are deploying AI agents that book supplier invoices, top up API credit balances, settle micro-transactions between services, rebalance treasury positions, and pay for compute resources, all without a human reviewing or approving each transaction individually. The agent is given a goal, a budget, and a set of rules, and it gets on with it.

This shift is being accelerated by several forces at once. Open banking regulations have made it technically straightforward for software to initiate payments via standardised APIs, without needing a human to log into a banking interface. Payment orchestration platforms now offer programmable

payment rails that are designed explicitly for machine callers. Cloud-native AI infrastructure means an agent can spin up, complete a task involving dozens of financial micro-transactions, and shut down again, all within minutes. And the economics of agentic AI make this attractive: human oversight of routine financial operations is expensive, slow, and error-prone compared to a well-governed agent following a defined policy.

The volumes involved are also changing the picture. A procurement agent handling supplier payments might execute several hundred transactions per working day. A financial services firm running algorithmic strategies through an agentic layer might see thousands. A marketplace platform settling payments between sellers and buyers via an orchestration agent might process millions of micro-transactions per month. These are not edge cases. They are the emerging normal for organisations that have moved their operational finance into the agentic layer.

None of this is necessarily a problem. Businesses have always used automated systems to initiate financial transactions, direct debits, standing orders, batch payment files. What is new is the degree of autonomy: the agent is making decisions, not just executing pre-approved instructions. And that autonomy is what creates the compliance challenge.

SECTION 2

What Makes an Agentic Payment Different

The conventional payment compliance model assumes a human originator: someone who decides to make a payment, authenticates themselves, and presses a button (or signs a form, or calls their banker). The compliance controls, identity verification, sanctions screening, transaction monitoring, suspicious activity detection, are calibrated against human behaviour patterns. Humans tend to make payments in recognisable contexts: paying known counterparties, at predictable times, in amounts that fit known salary or business patterns.

Agentic payments look different in almost every dimension that compliance systems use to assess risk:

- **Volume.** An agent operating a SaaS procurement workflow might initiate ten times more transactions per day than a human employee managing the same function. Volume spikes that would flag a human account as suspicious are routine for an agent operating at capacity.
- **Timing.** Agents do not respect business hours. A payment orchestration agent running in a cloud environment will make transactions at 3 am on a Sunday as readily as it does on a Tuesday afternoon. Many AML systems treat unusual timing as a risk indicator. For agents, there is no usual time.
- **Geography.** Agentic AI systems frequently interact with global API providers, cloud platforms, and international suppliers. A single agent might send payments to counterparties in fifteen different countries in a single day, a pattern that would trigger enhanced due diligence checks for a human customer.
- **Counterparty diversity.** Agents optimise for task completion, not for relationship familiarity. They will pay whichever supplier, API, or service best meets their criteria, which means the counterparty list may be broad and change frequently. Human transaction monitoring looks for unusual counterparties; everything is potentially unusual in an agent's payment history.
- **Decision autonomy.** When a human makes an unusual payment, there is generally a human decision behind it that can be retrieved and reviewed. When an agent makes an unusual payment, the decision was made algorithmically, and tracing it requires accessing the agent's reasoning log, something that may not exist in a compliance-readable format, or at all.

The result is that agentic payments strain conventional AML monitoring in two opposite directions simultaneously. The agent's normal behaviour looks suspicious by human standards, causing false positive alerts that waste investigator time. At the same time, genuinely suspicious patterns embedded within high-volume agentic activity are harder to detect because the baseline behaviour is already so far outside the human norm.

SECTION 3

The AML and KYC Gap

Anti-money laundering law in every major jurisdiction imposes obligations on financial institutions and, increasingly, on payment service providers, e-money institutions, and virtual asset service providers. The core obligations are consistent: know who your customer is, screen them against sanctions and watchlists, monitor their transactions for suspicious patterns, and report anything that looks like the proceeds of crime being moved, layered, or integrated into the legitimate financial system.

All of these obligations presuppose a customer who can, in principle, be known. KYC is literally "Know Your Customer", it assumes there is a customer, a person or legal entity, whose identity can be verified and whose beneficial ownership can be established. The customer due diligence process is designed to answer a set of questions about a human (or the humans behind a company): who are they, what is their source of funds, what is the expected pattern of their transactions, and do they appear on any relevant watchlists?

When an AI agent initiates a payment, it introduces a new layer between the human beneficial owner and the transaction. The immediate originator of the payment is software, a tenant ID, an API key, a service account. This is not a customer in any sense that traditional CDD frameworks anticipate. It has no name, no address, no date of birth, no nationality, and no source of funds in the conventional sense. It is an identity construct that exists only within the software environment.

The gap is this: the human or organisation that owns the agent, controls its budget, and is ultimately responsible for its actions is the real party of interest for AML purposes. But that beneficial owner may be several layers of delegation removed from the actual payment instruction. Between the human and the transaction sits the agent (which may itself delegate to sub-agents), the payment orchestration layer, the API gateway, and the payment service provider's interface. Each layer is a potential point where the link between transaction and beneficial owner can be lost or obscured, not through any intention to evade, but simply because the technical architecture was not designed with the AML attribution chain in mind.

> **The core problem:** Agentic payments break the assumption that the immediate payment originator and the beneficial owner are the same entity. Compliance frameworks need a reliable way to bridge the gap between the software that initiates the payment and the human or organisation that authorised it.

This gap also creates a second-order risk. If legitimate agentic payment flows are difficult to attribute to a beneficial owner, so are illegitimate ones. A money laundering scheme that uses an AI agent as the payment initiator gains a layer of indirection that makes beneficial owner tracing harder. The very architecture that makes agentic payments efficient also makes them attractive for anyone who wants to add opacity to a financial flow.

SECTION 4

Who Is the Customer?

This is the question that sits at the heart of agentic payment compliance, and it has a clear answer: the customer, for AML and KYC purposes, is always the human or legal entity that ultimately controls the funds being moved and authorised the agent to move them. The agent is a mechanism, not a party. This is the same principle that applies to corporate payment systems, automated batch payments, and direct debit mandates: the legal and regulatory responsibility lies with the entity that authorised the system, not with the system itself.

What changes with agentic payments is the complexity of the authorisation chain, and the speed at which it needs to be validated. In a conventional corporate payment setup, the authorisation chain is stable: the company has a bank account, the bank has performed CDD on the company, the company has authorised a small set of individuals to make payments, and each payment is reviewed or batch-approved by those individuals. The chain is short and changes slowly.

In an agentic payment setup, the authorisation chain may look like this: a human user grants a top-level agent permission to make payments up to a certain value for certain categories of expenditure. That agent spins up a sub-agent to handle a specific task. The sub-agent calls a payment API. The payment API calls the payment rail. At each step, the authority to make the payment was delegated, but the delegation happened in software, not in a compliance-readable document.

For an AML system to function correctly, it needs to be able to trace this chain on demand. Not in the sense that it reads every delegation log in real time, that would be impractically slow. But in the sense that if a transaction is ever investigated, the chain from payment to beneficial owner can be reconstructed with confidence, and the records supporting that reconstruction are tamper-resistant.

This requires an architecture that captures authorisation events cryptographically at each delegation step, not as an afterthought but as a core part of the payment flow design. The delegation record needs to exist, be readable, and be linked to both the KYC record of the beneficial owner and the transaction records of every payment made under that delegation.

SECTION 5

FATF, the Travel Rule, and Machine Payers

The Financial Action Task Force (FATF) sets the international standards that national AML frameworks are built on. FATF Recommendation 16, commonly known as the Travel Rule, requires that originator and beneficiary information travel with wire transfers above a threshold value (USD/EUR 1,000 in most implementations). The originator information must include the name, account number, and address of the person or entity sending the funds. This requirement exists so that every institution in a correspondent banking chain can screen the parties involved.

The Travel Rule was designed with human or corporate originators in mind. When the originator is an AI agent, the "name" available at the point of the transaction is the agent's technical identifier, a tenant ID, a service account

name, or an API credential. None of these are the originator information that FATF expects, because none of them identify the beneficial owner.

In 2019, FATF extended Travel Rule obligations to virtual asset service providers (VASPs). This extension brought cryptocurrency exchanges, stablecoin issuers, and digital asset platforms into scope. Many of these platforms are already primary environments for agentic payment activity, particularly in the decentralised finance (DeFi) space, where smart contracts and protocol agents initiate transactions autonomously. The extension of the Travel Rule to VASPs without explicit guidance on how it applies to automated transaction originators has left a significant implementation gap.

FATF's 2021 updated guidance on virtual assets acknowledged that "unhosted wallets" and automated transaction systems present challenges for Travel Rule compliance, but stopped short of providing a framework for how agentic originators should be handled. The practical implication is that VASPs and payment service providers operating in the agentic payments space must develop their own interpretations of how Travel Rule originator information should be constructed when the immediate payer is software.

REQUIREMENT	HUMAN ORIGINATOR	AGENT ORIGINATOR	WHAT'S NEEDED
Originator name	Full legal name	Tenant ID or service account	Link from agent ID to beneficial owner's legal name
Originator account	Account number or IBAN	API wallet or payment account	Payment account linked to KYC-verified entity
Originator address	Residential or registered address	Cloud endpoint or IP address	Registered address of the controlling entity
Sanctions screening	Name-matched at onboarding and transaction	Agent has no name to screen	Screen beneficial owner; proof travels with transaction
Audit trail	Bank records + CDD file	Agent logs (may not be compliance-readable)	Cryptographic delegation records linked to CDD

The direction of travel from regulators is clear, even without explicit guidance: beneficial owner traceability must be maintained regardless of whether a human or a machine initiates the transaction. The question is how to achieve this technically without creating a compliance process so burdensome that it makes agentic payments impractical.

SECTION 6

Where AffixIO's API Sits in the Flow

AffixIO's API operates as a verification and attestation layer between the agent's payment instruction and the payment execution. It does not process the payment itself. It provides the cryptographic proof that the payment was authorised by a KYC-verified beneficial owner, and it maintains the audit trail that links every agent transaction back to that beneficial owner.

The flow works in three stages.

Stage one: beneficial owner onboarding

When a new organisation or individual deploys an agent with payment capabilities, they go through a KYC process in the normal way, identity verification, sanctions screening, source of funds assessment, and any enhanced due diligence required by their risk profile. AffixIO's API converts the output of this KYC process into an eligibility proof: a cryptographic certificate that confirms the beneficial owner passed all required checks, without storing the underlying personal data. This follows the same PII-free KYC approach described in WP-006. The eligibility proof is issued to the organisation and linked to a tenant identity in AffixIO's system.

Stage two: agent authorisation

The organisation registers its payment agents with AffixIO's API. Each agent receives a delegation record: a cryptographically signed statement linking the agent's technical identifier to the beneficial owner's eligibility proof. The delegation record includes the scope of authority (what types of payments the agent is authorised to make, up to what value, for what period), the

beneficial owner's eligibility proof reference, and a validity period. If the delegation is revoked, because the agent is shut down, the agent's scope is changed, or the beneficial owner's KYC status changes, the revocation is recorded immediately and all subsequent agent payment requests referencing that delegation will fail the authorisation check.

Stage three: per-transaction attestation

When the agent initiates a payment, it calls AffixIO's API to generate a payment authorisation token. The token contains the agent's identifier, a reference to its delegation record, a timestamp, a hash of the payment instruction (not the payment data itself), and a zero-knowledge proof confirming that the beneficial owner's KYC eligibility is current and that the delegation is valid. This token travels with the payment instruction to the payment processor or financial institution. The receiving institution can verify the token against AffixIO's public API without accessing any personal data about the beneficial owner.

> **The key design principle:** AffixIO does not sit in the payment path. It sits in the authorisation path. The payment rails process the payment; AffixIO proves that the payment was authorised by someone whose identity has been verified to the required standard.

This architecture means that AffixIO's API can be integrated into any payment flow without changing the payment infrastructure itself. The payment processor receives an additional token alongside the payment instruction; it can choose to verify the token (if it has integrated AffixIO's verification endpoint) or pass it on to the next institution in the chain for verification at settlement or for regulatory reporting purposes.

SECTION 7

Proving Authorisation Without Storing It

The privacy challenge in agentic payments is the mirror image of the compliance challenge. The compliance requirement is that beneficial owner information be attributable to every transaction. The privacy requirement is that beneficial owner information not be exposed to every institution in the payment chain, or stored in every system that the payment passes through.

Conventional approaches to Travel Rule compliance handle this tension by sharing originator information through encrypted bilateral channels between Financial Institutions, protocols like IVMS101 and the various Travel Rule solutions built on it. These work reasonably well for human-originated wire transfers between established banking institutions. They work less well for agentic payments at high volume across heterogeneous payment environments, because they require each institution in the chain to have a bilateral relationship and data-sharing arrangement with every other institution.

AffixIO's approach uses zero-knowledge proofs to separate the proof of eligibility from the eligibility data itself. The payment authorisation token proves that the beneficial owner is verified and eligible without disclosing who the beneficial owner is or what their personal data contains. Any institution that receives the token can verify its validity (the beneficial owner passed KYC, the agent has valid delegation, the delegation has not been revoked) without accessing any personal data.

The personal data itself remains with the organisation that performed the KYC, typically the institution that onboarded the beneficial owner as a customer, and is available to competent authorities on request through the normal legal process. The ZK proof approach does not eliminate the ability of regulators to access beneficial owner information in an investigation; it ensures that this access happens through the appropriate legal channel rather than being embedded in every transaction record that passes through the payment system.

For the agent operator, this means that deploying a payment agent does not require building a complex, bilateral data-sharing infrastructure with every payment counterparty. The authorisation token is self-contained and

verifiable by any party with access to AffixIO's public verification endpoint. The compliance overhead of adding a new payment counterparty is minimal: the counterparty receives the same token structure as every other counterparty; there is nothing to configure bilaterally.

SECTION 8

Audit Trails That Regulators Can Follow

A common concern about novel compliance architectures is whether they produce records that regulators will actually accept. The traditional KYC file, a collection of scanned documents, check results, and case notes stored in a compliance management system, is well understood by financial regulators. A cryptographic proof stored in a Merkle tree is not, at least not yet.

AffixIO's audit trail is designed to be readable and traceable by anyone familiar with basic digital record-keeping, even if they are not familiar with the underlying cryptographic technology. Each authorisation event generates a governance record that contains the following information in plain terms: when the event happened (timestamp), which agent made the request (agent identifier), what the agent was authorised to do (delegation scope), whether the beneficial owner's KYC was current at that time (eligibility proof status), and what the outcome was (authorised or denied).

These records are anchored in a Merkle tree, a type of data structure that makes it mathematically verifiable that a record has not been altered since it was created, and that all records within a given period are present and accounted for. Each record is also signed with a post-quantum digital signature (ML-DSA-65, per NIST FIPS 204), ensuring that the signatures remain valid against future computing advances and that the records cannot be quietly rewritten over a five-to-ten year regulatory retention period.

From a regulator's perspective, the audit trail provides the following investigative capabilities:

- **Transaction attribution:** given a transaction reference, retrieve the authorisation token that accompanied it, confirm the agent that made it

and the delegation record it operated under.

- **Delegation tracing:** follow the delegation chain from the payment-initiating agent back through any intermediate delegation levels to the beneficial owner's KYC eligibility proof.
- **Temporal verification:** confirm that the agent's delegation was valid at the precise moment of the transaction, and that no revocation was in effect at that time.
- **Completeness verification:** confirm that every agent transaction in a given period has a corresponding authorisation record, without needing to read the content of those records.

The last point is particularly important for large-scale agentic payment operations. A compliance examination that needs to verify that ten thousand agent transactions all had valid authorisation does not require reading ten thousand individual records. The Merkle tree structure allows the examiner to verify that the set of records is complete and unaltered in a single mathematical check. Individual records can then be sampled for content review as required.

SECTION 9

AML Screening at Agent Speed

Transaction-level AML screening, checking each payment against a sanctions list and submitting it for transaction monitoring review, was designed for human-volume payment flows. At agent volumes, the economics of per-transaction screening break down rapidly. An agent making two hundred transactions per day cannot practically pause each one for a human review step that might take minutes or hours. The agent would grind to a halt. The benefit of agentic payments, speed and scale, would be negated by a compliance process designed for a slower world.

AffixIO's approach shifts the primary AML screening burden from the per-transaction level to the onboarding and refresh level. The beneficial owner is screened comprehensively at onboarding: sanctions lists, PEP (Politically

Exposed Person) lists, adverse media, and any jurisdiction-specific watchlists. The result of this screening is incorporated into the eligibility proof. When the proof is issued, it reflects a clean screening result at that point in time.

The eligibility proof has a validity period. Within that period, agent transactions referencing the proof can proceed without a repeated full sanctions re-screen of the beneficial owner. The operator is responsible for configuring a validity period that reflects their risk assessment and regulatory obligations, a higher-risk customer category might warrant a shorter proof validity period and more frequent re-screening; a lower-risk category might sustain a longer validity period.

Critically, continuous sanctions list monitoring remains in place. AffixIO's platform monitors for changes to the relevant sanctions lists and, if a previously clear beneficial owner is added to a list, immediately revokes all delegation records linked to that beneficial owner. Agent payment requests referencing a revoked delegation are blocked at the authorisation stage, before the payment reaches the payment rail. The revocation is immediate, there is no window during a refresh cycle where a newly sanctioned beneficial owner's agent continues to make payments.

Per-transaction monitoring for behavioural anomalies, velocity spikes, unusual geographic patterns, unexpected counterparty types, continues to operate at the transaction level, but against a baseline that is calibrated to the agent's expected behaviour rather than to a human's. AffixIO's governance records provide the data that allows anomaly detection to be tuned to agentic patterns. An agent that suddenly begins making payments to counterparty types outside its defined scope, or at a velocity significantly above its established pattern, generates an alert, not because it is behaving like a suspicious human, but because it is behaving outside its own established parameters.

SECTION 10

The Regulatory Horizon: PSD3, MiCA, and Beyond

The regulatory environment for agentic payments is moving quickly, and in a consistent direction. Several legislative and regulatory developments are converging on the same conclusion: beneficial owner traceability must be preserved in automated and autonomous payment systems, and payment service providers must be able to demonstrate that their systems support this regardless of whether payments are initiated by humans or machines.

PSD3 and the Payment Services Regulation

The European Union's proposed Payment Services Directive 3 (PSD3), accompanied by the Payment Services Regulation (PSR), explicitly addresses automated payment initiation and the requirements for payment service providers handling API-initiated transactions. The legislative proposals require that strong customer authentication frameworks extend to non-human initiators in ways that preserve accountability, and that consent and delegation frameworks in open banking APIs must support attribution of a payment to the natural person or legal entity whose funds are being moved. While PSD3 is primarily addressed at the open banking infrastructure layer, its requirements flow directly into the compliance architecture for any agentic payment system operating on European payment rails.

MiCA and virtual assets

The Markets in Crypto-Assets Regulation (MiCA) establishes obligations for crypto-asset service providers (CASPs) operating in the European Union, including Travel Rule obligations for transfers of crypto-assets above threshold. MiCA's Travel Rule provisions adopt the FATF standard and require that originator and beneficiary information travel with crypto-asset transfers. For agentic payment flows involving stablecoins, tokenised deposits, or other MiCA-regulated crypto-assets, compliance with MiCA's Travel Rule requires the same beneficial owner attribution capability that applies to conventional wire transfers.

UK and US developments

In the United Kingdom, the Payment Systems Regulator and the Financial Conduct Authority have both signalled that firms deploying AI in payment and financial services contexts are expected to maintain the same standards of transparency and accountability that apply to human-operated systems. The FCA's consumer duty framework requires that firms operating AI-mediated services can demonstrate fair treatment and identifiable accountability. The Treasury's AI in financial services roadmap, published in 2025, explicitly referenced the need for audit trail requirements to be technology-neutral, applicable to AI agent systems as much as to conventional systems.

In the United States, FinCEN's ongoing rulemaking on beneficial ownership (implemented under the Corporate Transparency Act) and its separate work on AI in financial services both point towards a compliance environment in which the use of AI or automated systems in payment flows is not a reason to reduce transparency requirements but an incentive to increase them. The Bank Secrecy Act's requirements for customer identification, suspicious activity reporting, and record retention apply regardless of whether a human or a machine initiates the underlying transaction.

The common thread

Across all of these regulatory developments, the direction is consistent: beneficial owner attribution, real-time revocation capability, and tamper-resistant audit trails are baseline requirements for any payment architecture, agentic or otherwise. The organisations that will navigate this landscape most successfully are those that build these capabilities into their agentic payment infrastructure from the start, rather than attempting to retrofit them onto systems that were not designed with compliance in mind.

SECTION 11

What Doesn't Change

It is worth being clear about the boundaries of what AffixIO's approach changes, because some elements of AML compliance are not affected by the introduction of agentic payments and should not be treated as though they are.

Suspicious activity reporting obligations remain unchanged. If an organisation's compliance team identifies a suspicious pattern in its agent's payment activity, unusual counterparties, transactions that lack business rationale, patterns consistent with layering or integration, the obligation to file a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) is unchanged. AffixIO's governance records provide better data for making these determinations; they do not reduce or remove the obligation to make them.

Customer due diligence on counterparties remains unchanged. The beneficial owner of the agent's payments needs to be verified; so do the counterparties receiving those payments, where the applicable regulations require it. AffixIO's approach addresses the originator side of the transaction; counterparty due diligence obligations are unchanged and remain the responsibility of the receiving institution.

Enhanced due diligence for high-risk scenarios remains unchanged. If the beneficial owner of an agent falls into a high-risk category, a Politically Exposed Person, a customer in a high-risk jurisdiction, a business in a sector with elevated money laundering risk, enhanced due diligence requirements apply to their agent's payment activity as much as to their own direct transactions. The eligibility proof mechanism can reflect enhanced due diligence status, but it does not remove the underlying obligation to perform that due diligence to the appropriate standard.

Governance and accountability within the organisation remain unchanged. The organisation deploying the agent is responsible for its agent's compliance. If the agent makes a payment that turns out to be to a sanctioned counterparty because the agent's counterparty screening was inadequate, the organisation bears the regulatory consequences, not the agent. AffixIO

provides the proof of the beneficial owner's eligibility and the authorisation chain; the organisation remains responsible for the configuration and oversight of what the agent is authorised to do and with whom.

These continuities matter because there is a risk that "agentic compliance" is presented as a more sophisticated version of compliance that supersedes conventional obligations. It does not. It is an adaptation of conventional obligations to an environment where payments are initiated by software. The obligations themselves remain exactly as they were designed: to prevent the financial system from being used to move the proceeds of crime.

SECTION 12

Conclusion

Agentic payments are not a future scenario. They are a present reality in corporate treasury, API-driven businesses, open banking applications, and decentralised finance. The compliance frameworks designed for human-initiated payments do not map cleanly onto software-initiated payments, and the gap between the two is a real risk, both for the organisations deploying agents without adequate compliance infrastructure, and for the financial system as a whole if that gap is exploited.

The solution is not to slow agents down to human speed so that conventional compliance controls can apply. The solution is to provide the compliance controls that work at agent speed: pre-verified beneficial owner eligibility, cryptographic delegation records that link every agent transaction to an identifiable authorising party, real-time revocation when eligibility changes, and tamper-resistant audit trails that regulators can trace and examiners can verify.

AffixIO's API provides this layer. The beneficial owner is verified once at onboarding, through whatever KYC process their risk profile requires. The eligibility proof travels with every subsequent agent transaction, without carrying the personal data it represents. The Merkle-anchored audit trail

records every authorisation event in a form that is tamper-resistant, post-quantum secure, and readable by any compliance team or regulatory examiner without specialist cryptographic knowledge.

The regulatory horizon is clear. PSD3, MiCA, FATF guidance updates, and national supervisory expectations are all converging on the same requirement: beneficial owner traceability at machine speed, with audit trails that last as long as the regulations require. AffixIO is built to provide exactly that. For organisations that are building agentic payment capabilities today, the time to integrate compliance infrastructure is now, before the agent has run ten thousand transactions, and before a regulatory examination discovers that the authorisation chain was never captured.

Related reading

- WP-006: A PII-Free KYC Schema by Design: Structural Data Minimisation via Zero-Knowledge Identity Circuits
- WP-015: Agentic AI Governance with ZK Proof Chains
- WP-014: Double-Spend Prevention for Zero-Knowledge Proofs
- WP-020: DORA, MiCA, and AI Governance: Overlapping Obligations for Financial Firms

Frequently asked questions

Who counts as the customer when an AI agent makes a payment?

For AML purposes, the relevant party is always the human or legal entity that authorised the agent, the beneficial owner of the funds. The agent is the mechanism; the beneficial owner is the customer. AffixIO's delegation records maintain this link cryptographically from every payment back to the verified beneficial owner.

Does the FATF Travel Rule apply to machine-to-machine payments?

FATF Recommendation 16 applies based on the nature of the transaction and the thresholds involved, not on whether a human or machine initiates it. Agentic payments above threshold require originator and beneficiary information regardless of how they were triggered. AffixIO's payment authorisation token carries the originator attribution information in a verifiable form.

How does AffixIO's API fit into an agentic payment flow?

AffixIO sits in the authorisation layer: the beneficial owner is KYC-verified at onboarding, generating a reusable eligibility proof. Every subsequent agent payment carries a reference to that proof and a delegation token, giving payment processors and compliance teams a verifiable audit trail without repeating the full KYC check each time.

What happens if a beneficial owner is added to a sanctions list after their agent is already running?

AffixIO monitors the relevant sanctions lists continuously. If a beneficial owner is added to a list, all delegation records linked to that owner are immediately revoked. Agent payment requests referencing a revoked delegation are blocked at the authorisation stage, before the payment reaches the payment rail.