PAYJOIN FOUNDATION *Infrastructure Partner Brief*

Run Payjoin Infrastructure

Deploy lightweight, zero-custody infrastructure that strengthens
Bitcoin privacy for everyone

What Is Payjoin Mailroom?

`payjoin-mailroom` is a single, lightweight binary that bundles the two server-side roles required by Async Payjoin (BIP 77):

- **Payjoin Directory**: a store-and-forward mailbox that holds small, ephemeral, end-to-end encrypted payloads so a sender and receiver can complete a payjoin asynchronously (they don't need to be online at the same time).
- **OHTTP Relay**: a simple HTTP proxy that separates client IP addresses from the directory, preventing the directory from correlating users with their network identity. No loopbacks between the relay and directory within the same instance.

Together, these two components are the backbone that makes Async Payjoin work for *every* wallet.

Why Does This Matter?

Payjoin breaks the most damaging assumption in on-chain surveillance: that all inputs to a transaction belong to one person. By letting sender and receiver batch into a single transaction, payjoin makes chain analysis dramatically harder, and unlike mixing, Payjoin looks like any typical transaction.

Async Payjoin removed the last barrier to adoption: receivers no longer need to run servers. But this convenience depends on directory and relay infrastructure existing. Today, only a small handful of operators run these services. A single point of failure is a single point of censorship.

Why Does It Matter Who Runs This?

Bitcoin privacy infrastructure works best when it's operated by entities that can sustain it long-term. The ideal operators are organizations with the resources, jurisdiction, and institutional will to keep infrastructure online: companies with legal counsel, organizations in privacy-respecting jurisdictions, and entities with a track record of supporting open-source infrastructure.

We don't need a sprawling network of operators. Fewer directories means a larger anonymity set: the more users share a single directory, the harder traffic analysis becomes. But we do need **a few more resilient operators** for redundancy and resistance to censorship.

Trust Model: YOU SEE NOTHING

All payjoin payloads are end-to-end encrypted with HPKE. The directory cannot read, forge, or correlate transaction contents. The OHTTP relay only sees encrypted blobs and never learns who is paying whom. No loopbacks between relay and directory roles.

You never touch bitcoin. You never see transactions. Zero custody risk.

What You Need

REQUIREMENT	DETAILS
Server	A $5/month VPS is sufficient. Minimal CPU and RAM.
Domain + TLS	A domain name with a valid TLS certificate (Let's Encrypt works).
Storage	Very minimal. Only HPKE key material and config are persisted. Payjoin payloads are ephemeral.
Deployment	Docker image, Nix flake, or build from source. Inline config supported.
Bitcoin Node	**Not required.** Pure relay infrastructure. No chain access needed.

FAQ

Can the operator steal or censor bitcoin?

No. The service never holds keys, constructs transactions, or accesses a bitcoin node. All payloads are encrypted end-to-end. The worst an operator can do is go offline, in which case wallets automatically fall back to the typical (non-payjoin) transaction included in the BIP 21 URI. No funds are ever at risk.

What is the service comparable to, architecturally?

Think of a CDN or encrypted email relay. You forward opaque, encrypted blobs between parties. You cannot inspect, modify, or correlate the contents. Even a fully compromised operator learns nothing useful.

What about OFAC compliance?

Async Payjoin sessions are encrypted end-to-end and opaque by design, so payload-level screening is not possible. payjoin-mailroom applies configurable IP address filtering to all requests regardless of protocol version. For optional v1 backwards-compatibility (plaintext), the service can also screen Bitcoin addresses directly. Operators can enforce their own compliance policies without any changes to the protocol.

What data does the operator see?

Aggregate metrics only: raw mailbox counts (roughly two per payjoin session). The operator never sees payload contents, Bitcoin addresses, or sender/receiver identity. OHTTP blinds client IP from the directory, and all payloads are encrypted end-to-end. This is less visibility than even Signal has running their own infrastructure, since Signal registers phone numbers and sees payload sizes. payjoin-mailroom does neither.

Is there a revenue model?

Public-good infrastructure. Running a mailroom is a reputation signal that your organization takes Bitcoin privacy seriously. The spec includes optional DoS-prevention auth tokens for the future, but current load is minimal.

Who uses this infrastructure today?

Bull Bitcoin (first mobile wallet with Async Payjoin send + receive), Cake Wallet, and the payjoin-cli reference implementation all depend on this infrastructure, with more integrations in progress. The flagship directory is payjo.in, with OHTTP relays run by a few community members.

Get Started

github.com/payjoin/rust-payjoin/tree/master/payjoin-mailroom

Questions? Reach out at payjoin.org or open a Discussion on GitHub.