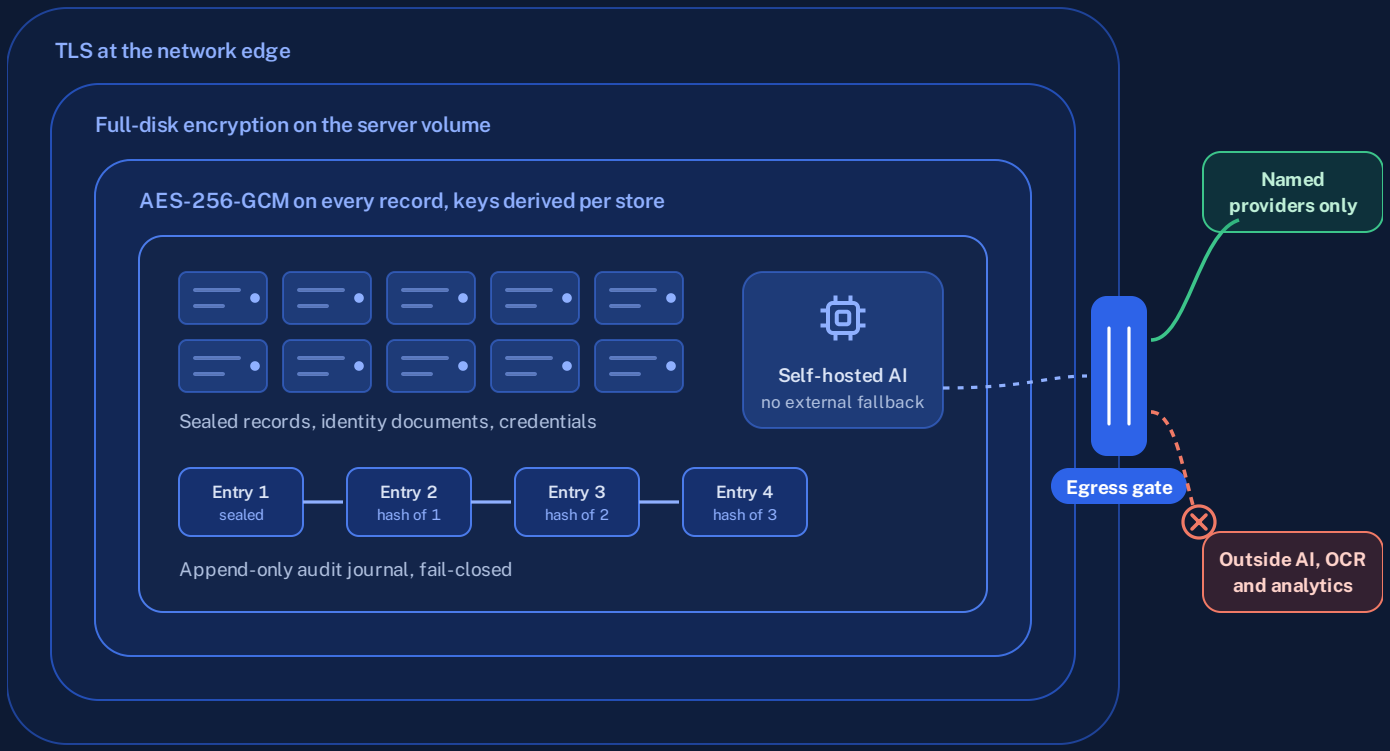
GOODFORUS

Government & public sector capabilities catalog

Payments and security built for public institutions.

One application. One console. Collections, disbursements, cards and compliance, on infrastructure we own and operate.

- AES-256 encryption at rest, on our own servers
- Append-only audit trail, 5-year retention (31 CFR 1010.430)
- Self-hosted AI: records never leave our walls



The company behind GoodForUs.

GoodForUs is built and run by SolutionsAe, Inc., an 8(a)-certified, HUBZone, woman-owned small business incorporated in Georgia in 1997 and federally registered since 2006, with roughly $20.4M in contract performance across 24 awards.

DM2JMC1SNNA3	4JQU3	124663969	Active
Unique Entity ID (UEI)	CAGE code	DUNS	SAM.gov registration, district GA-04

Certifications

- SBA 8(a) Certified
- HUBZone
- WOSB
- EDWOSB
- Small Disadvantaged Business
- Minority-Owned
- SDVOSB Mentor
- DBE: GA, FL, LA, WI, AL

NAICS codes

522320	**Financial transactions processing**
541511	Custom computer programming
541512	Computer systems design
541513	IT facilities management
541519	Other computer related services

Contract vehicles

GSA Multiple Award Schedule	**47QTCA18D00KU**
Schedule SINs	**54151S · OLM**
Governmentwide acquisition contract	**8(a) STARS III**



Points of contact

Dr. Ana Everett
President & Chief Executive Officer
(404) 518-7767 · team@solutionsae.com

Jake Brice
Business Development
904-501-8122 · jakebrice@solutionsae.com

Past performance

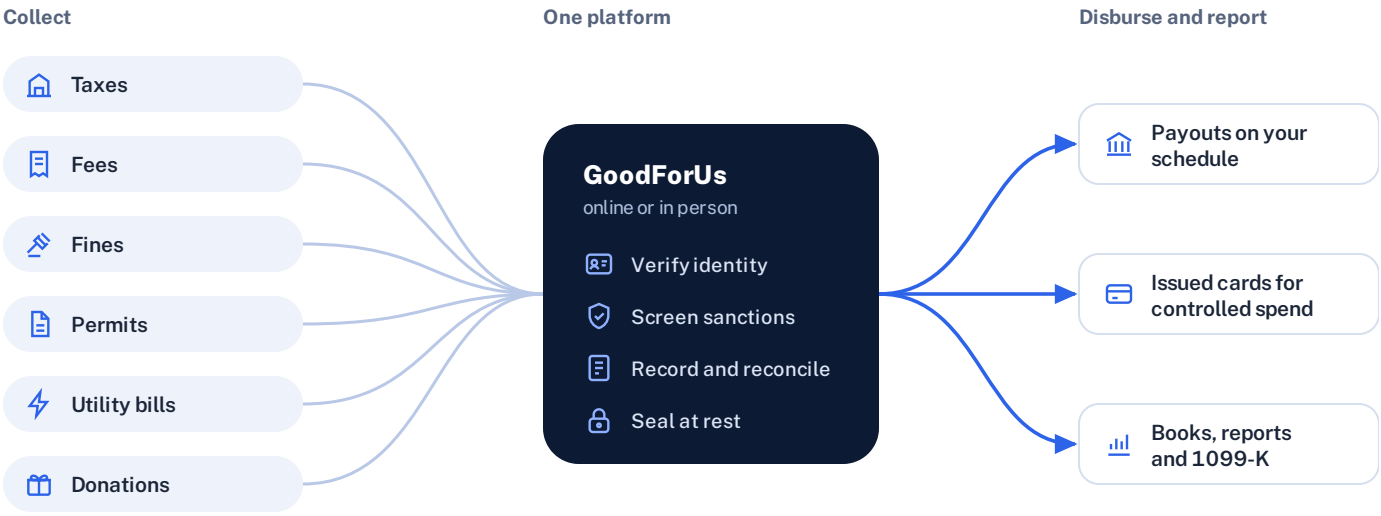
Twenty-four awards across six capability areas, $20,440,258 in total.

Emergency response and human services	**$7,914,985**
Deployment sanitization and environmental	**$7,483,000**
Highway and guardrail maintenance	**$4,037,833**
IT service management (HHS / CDC)	**$477,000**
Transportation and logistics	**$318,440**
Construction support	**$209,000**

Federal values are total obligations recorded in federal award data. Highway, transportation and construction values are contract values from company records; these are state, commercial and subcontract engagements and do not appear in federal award databases. Detail on any line is available on request.

Public money movement, built as one platform.

GoodForUs is a payment gateway and facilitator engineered for the way public institutions actually handle money: many kinds of inbound collection, disbursements on a schedule the agency sets, issued cards for controlled spend, and a complete, auditable record of every movement. Identity verification, sanctions screening, role-based access control and tamper-resistant record-keeping are part of the platform, not purchased as separate products, and everything runs on infrastructure GoodForUs owns and operates. This catalog sets out, capability by capability, what the platform does and how each piece maps to the control objectives government buyers evaluate against.



1	AES-256	5 yr	0
application to every rail	records sealed at rest	audit-log retention	outside data stores

Collect every kind of payment

Taxes, fees, fines, permits, utility bills and donations, online or in person. Each payment is categorized and reconciled against the rail, so a bank line always ties to a record.

Disburse on your schedule

Funds settle to an available balance you control, with maturity holds, per-item reserves and payouts your authorized staff approve, plus issued cards for controlled operational spend.

Security held to a public standard

Records sealed with AES-256 on servers we operate, money actions behind a second factor, and every change written to a fail-closed audit trail retained five years.

Compliance already on

Identity and business verification, OFAC sanctions screening, SAR tooling and a governance wall over regulated data come with the account, not as an add-on.

The standard, and how we meet it.

Public-sector procurement measures a payments platform against control objectives drawn from NIST SP 800-53, PCI DSS, the Bank Secrecy Act and related rules. Each objective below is stated in plain terms beside exactly how GoodForUs meets it. Every control listed is implemented and enforced in the production platform today.

Control area	Government standard & requirement	What GoodForUs provides	
Data protection	NIST SP 800-53 SC-28 PCI DSS Req 3 Protect stored data; render sensitive data unreadable wherever it is kept.	Datastore records, identity documents and stored credentials are each sealed with AES-256-GCM, and the server volume itself is encrypted at rest at the disk layer. The platform refuses to store a secret unless its encryption key is present.	✓
Data in transit	NIST SP 800-53 SC-8 PCI DSS Req 4 Encrypt sensitive data while it moves across open or public networks.	Transport is secured with TLS at the network edge; session cookies are issued secure in production.	✓
Logging and monitoring	NIST AU family PCI DSS Req 10 31 CFR 1010.430 Record access and changes to an audit trail and retain it for the required period.	An append-only, fail-closed audit journal records every money action and record change, retained five years and streamable to your SIEM. Agreement and decision records are additionally hash-chained.	✓
Authentication	NIST IA family PCI DSS Req 8 Require multi-factor authentication for system access and sensitive actions.	Time-based one-time passwords (RFC 6238) and SMS second factors, with step-up re-authentication on sensitive money actions such as changing a payout bank account.	✓
Access control	NIST AC family PCI DSS Req 7 Restrict access by role; enforce least privilege and separation of duties.	Capability-based roles grant only what each job needs. Payouts and bank-account changes move through request-and-approval by a different, authorized person.	✓
Boundary and residency	NIST SP 800-53 SC-7 Monitor and control communications at external system boundaries.	Every outbound connection passes a single egress gate. Outside OCR, analytics, logging and AI are hard-blocked; agency data stays on infrastructure we operate.	✓

Control area	Government standard & requirement	What GoodForUs provides	
Identity program	31 CFR 1020.220 (CIP) · GLBA Verify the identity of customers and protect nonpublic personal information.	KYC/KYB verification feeds a declared governance wall; regulated identity data is usable for compliance only, never for analytics or personalization, even with consent.	✓
Data minimization	NIST SP 800-53 PT/DM · Privacy Act principles Collect and retain only the personal data that is necessary for the purpose.	A driver's license barcode is read, then deleted; the front image is kept only until the decision. What survives is the compliance result, not the raw identity document.	✓
Sanctions and AML	OFAC · Bank Secrecy Act (AML) Screen parties against sanctions lists, monitor for illicit activity and file reports.	Automated screening against the official OFAC SDN and Consolidated lists, with near-matches routed to a human reviewer, plus SAR tooling and PEP and adverse-media monitoring.	✓
AI and third-party data	CJIS-aligned handling · Agency data-sharing limits Do not expose sensitive data to uncontrolled third-party processors or models.	The platform's AI is self-hosted with no external fallback; no outside OCR, analytics or AI service ever receives agency data.	✓
Records retention	31 CFR 1010.430 (BSA) Retain required records for five years and protect them from premature deletion.	Five-year retention is enforced in code; the purge routine refuses to delete anything inside the retention window.	✓

Framework references indicate the control objective GoodForUs is designed to satisfy. Formal third-party attestation is pursued with sponsoring agencies as an engagement proceeds.

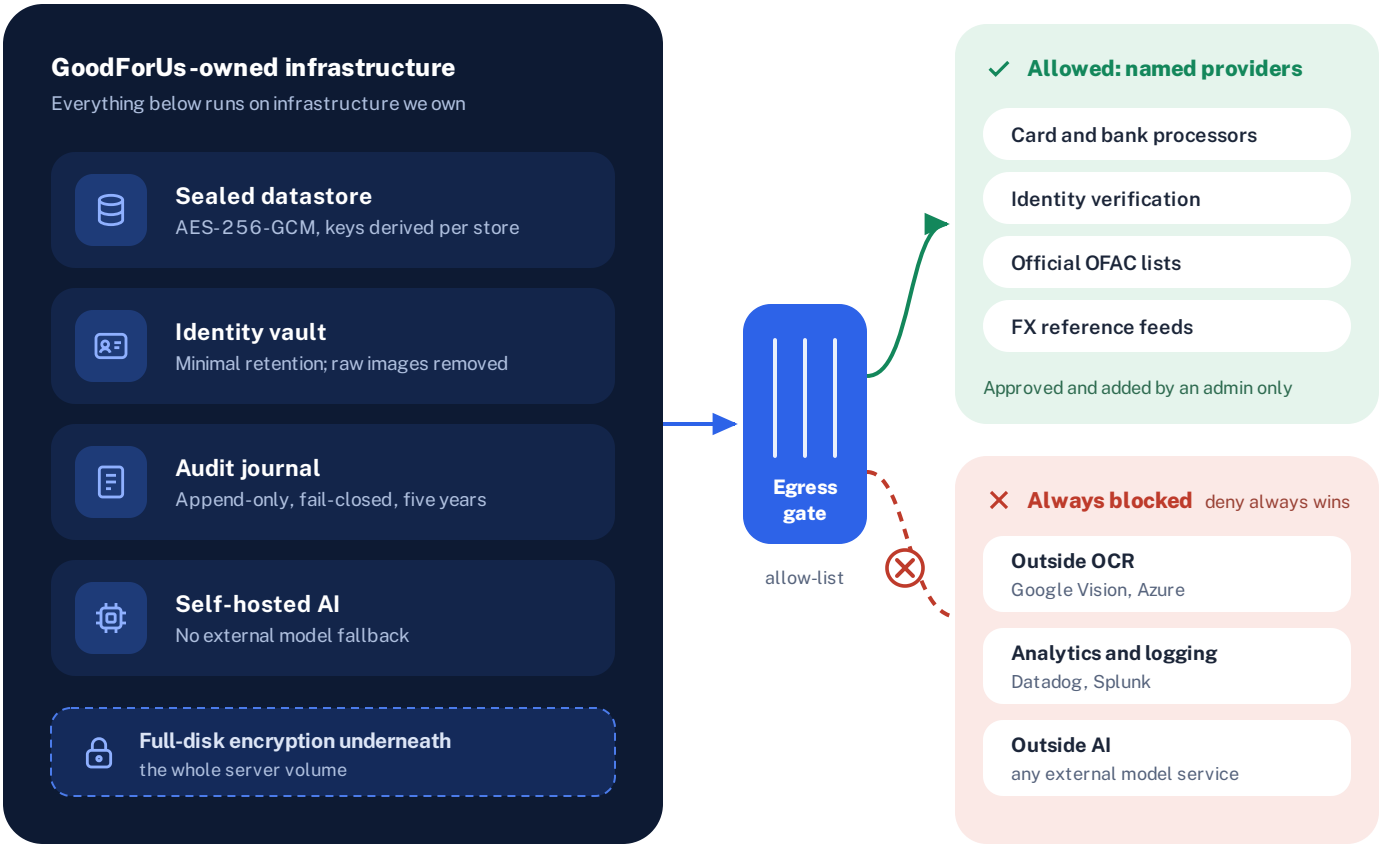
Coverage at a glance

Which frameworks each control area answers to, as referenced in the tables above.

Control area	NIST SP 800-53	PCI DSS	BSA / 31 CFR	OFAC	GLBA	Privacy Act	CJIS / agency data-sharing
Data protection	●	●	○	○	○	○	○
Data in transit	●	●	○	○	○	○	○
Logging and monitoring	●	●	●	○	○	○	○
Authentication	●	●	○	○	○	○	○
Access control	●	●	○	○	○	○	○
Boundary and residency	●	○	○	○	○	○	○
Identity program	○	○	●	○	●	○	○
Data minimization	●	○	○	○	○	●	○
Sanctions and AML	○	○	●	●	○	○	○
AI and third-party data	○	○	○	○	○	○	●
Records retention	○	○	●	○	○	○	○

Your data stays inside our walls.

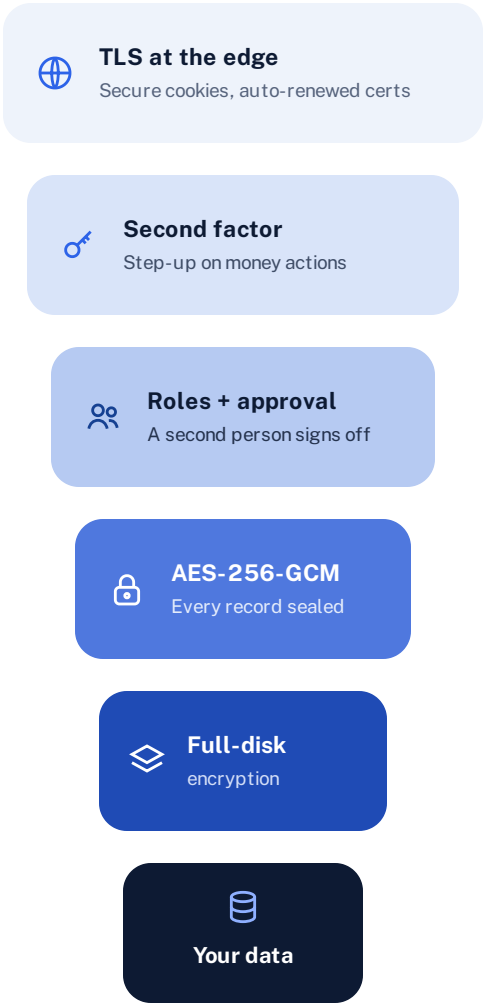
Public institutions cannot treat the location of their data as an afterthought. GoodForUs is built on a simple principle: agency and constituent data stays inside infrastructure GoodForUs owns and operates, and the only way out is through a single, audited gate. There is no analytics pixel, no outside logging service, no third-party document reader quietly holding a copy. What enters the platform stays in the platform unless it is sent, deliberately, to a named provider that is contractually required not to retain it.



For a buyer, the data-residency question has a short answer: it is on our servers. The egress gate is enforced in the shipped platform, and the block-list cannot be configured away; even a misconfiguration cannot send a constituent record to an outside store that would keep it.

Encrypted, logged, authenticated.

Protection comes in layers. A request has to clear each one on the way in, and every money action is written to the audit journal along the way.



Outside in: what a request has to clear

Encryption at rest

Every record the platform keeps is sealed before it is written to disk. The datastore, identity documents and stored credentials are each encrypted with AES-256-GCM under keys derived separately for each store, and the platform will refuse to persist a secret at all if its key is not present; there is no unencrypted fallback path. Beneath that, the server's disk is itself encrypted at rest, so data is protected at both the application and the storage layer.

Encryption in transit

Traffic is protected with TLS at the network edge, and in production session cookies are marked secure so they are never sent in the clear. Certificates are renewed automatically.

Tamper-resistant audit trail

Every money action and record change is written to an append-only journal that fails closed: if the write cannot complete, the action is rolled back rather than lost. The journal is retained for five years in line with 31 CFR 1010.430 and can be streamed to your SIEM. Agreement acceptances and underwriting decisions are additionally sealed and hash-chained, so any later alteration is detectable.



Strong authentication with step-up

Accounts use time-based one-time passwords (RFC 6238) or SMS as a second factor. Sensitive money actions, such as changing a payout bank account, rotating recovery codes or approving a deployment, demand a fresh step-up challenge, so a stolen password alone is never enough to move money or change where it goes.

Security, by the specifics.

A reviewer-facing summary of the controls implemented in the platform. Every item below is in force in the shipped production system.

Encryption at rest

- AES-256-GCM authenticated encryption on datastore records, identity-document blobs, stored payment and bank credentials, the license number, agreement signing keys, and backups.
- The platform refuses to persist a secret if its encryption key is absent; there is no plaintext fallback path.
- Keys derived per store via HKDF from configured secrets; held in environment or secret configuration, never in the datastore.
- The underlying server volume is encrypted at rest (full-disk encryption enabled on the host), protecting stored data at the disk layer in addition to the application layer.

Encryption in transit

- TLS terminated at the network edge (reverse proxy) with automated certificate renewal.
- Session cookies issued Secure in production.

Audit and logging

- Append-only, fail-closed journal: a write that cannot complete rolls back the action rather than losing the record.
- Five-year retention (31 CFR 1010.430); the purge routine refuses to delete inside the window.
- Streamable to an external SIEM. Agreement acceptances and underwriting decisions are additionally hash-chained (tamper-evident).

Authentication

- TOTP (RFC 6238) and SMS second factors; passkey step-up supported.
- Step-up re-authentication required on sensitive money actions (bank-account change, recovery-code rotation).
- Recovery codes are single-use and stored only as SHA-256 hashes; one-time-password replay is rejected.

Access control

- Capability-based role matrix; least privilege by default.
- Staff-management and access-management capabilities are locked to administrators.
- Payouts and bank-account changes move through request, then approval by a different, authorized person.

Boundary and data residency

- Single egress choke-point: default-deny allow-list of named providers; deny-list hard-blocks outside OCR, analytics, logging and AI.
- Datastore and document blobs are stored on local disk, with no third-party object store.
- Platform AI is self-hosted on GoodForUs infrastructure with no external model fallback.

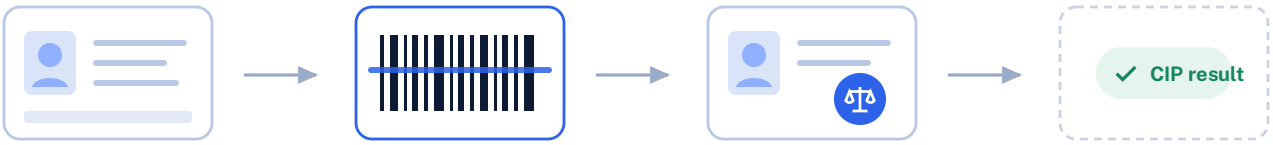
Enforced in the shipped production image

Encryption, the egress wall, the first-login agreement gate, the data-governance wall and the access controls above.

Verify fully. Keep almost nothing.

GoodForUs verifies who it is dealing with to the standard a regulated money program requires, then keeps as little of the result as the rules allow. Regulated identity data sits behind a declared governance wall: it is available for compliance and nothing else, not analytics, not personalization, not product improvement, even where a person has given consent.

The life of an identity document

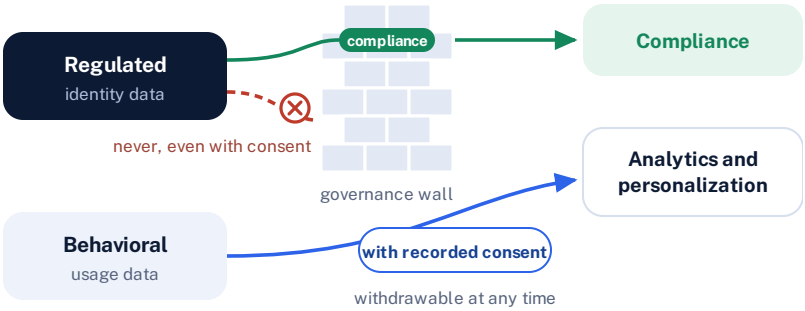


Capture	Read and verify	Decide	Minimize
Applicant submits ID	PDF417 barcode decoded	Match assessed	Raw image removed



A governance wall over regulated data

KYC/KYB checks classify each data kind as regulated, behavioral or operational. Regulated data is walled off for compliance use only; behavioral use requires recorded, withdrawable consent in the account.



Business and beneficial-owner verification

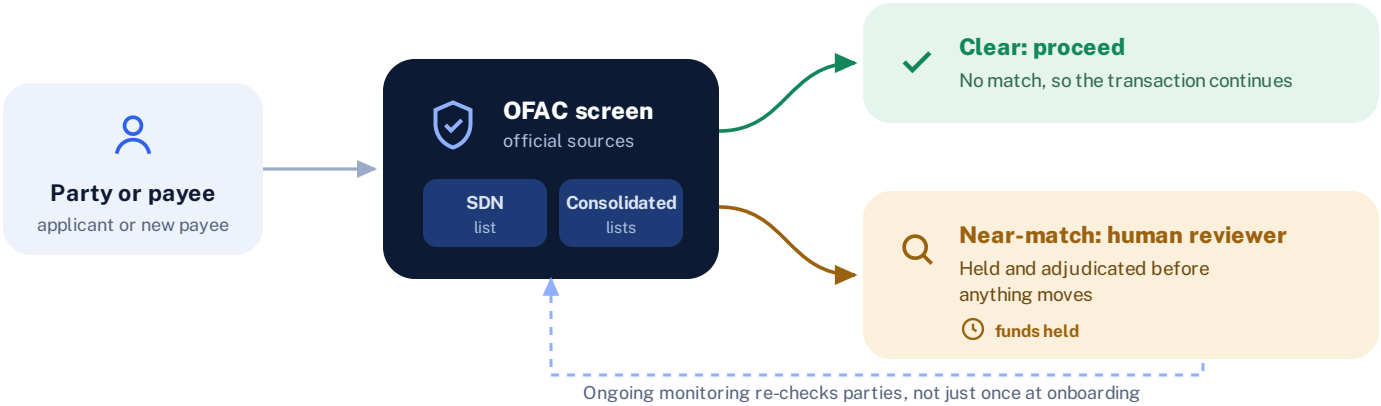
Organizations are verified as businesses, not just as a name: registration, ownership and the people authorized to act are checked before an account can move money.

- Registration checked
- Beneficial owners checked
- Authorized people checked
- Account can move money

Screened against the real lists.

Every party is screened against the official U.S. Treasury OFAC sanctions lists. The screen is automated and runs from authoritative sources; a clear result lets the transaction proceed, and a possible match is held and routed to a trained human reviewer who adjudicates it before anything moves. Nothing is auto-cleared past an unresolved sanctions flag.

Sanctions screening workflow

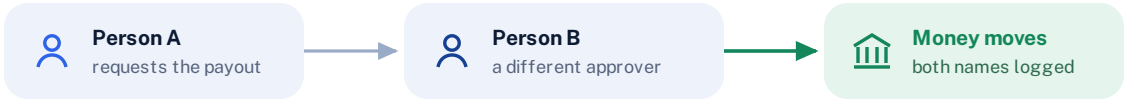


PEP and adverse-media monitoring

Beyond sanctions, politically-exposed-person and adverse-media signals are surfaced for review, and ongoing monitoring re-checks parties rather than screening once at onboarding.

Separation of duties on money actions

Capability-based roles enforce least privilege. A payout or a bank-account change is requested by one authorized person and approved by a different one, and every action is attributable to a named operator in the audit trail.



The requester can never approve their own request.

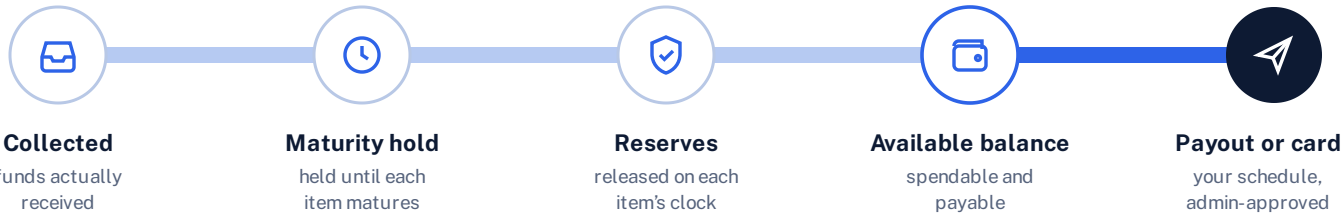
SAR tooling and case management

Suspicious-activity reporting and risk-case tooling are built in, so an escalation is recorded, worked and retained alongside the transactions it concerns.

Collect, settle, disburse.

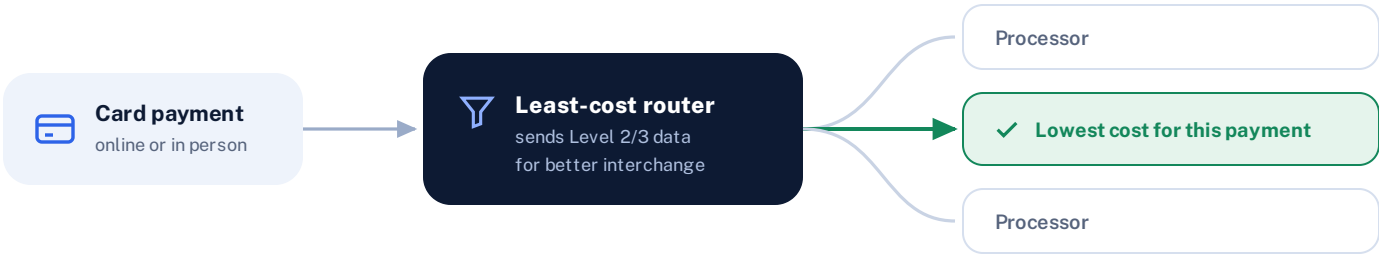
Only money actually collected is payable. Every dollar moves through the same stages, on its own clock, and leaves only on a schedule your administrators approve.

Settlement lifecycle



Scoped holds require a different administrator to release

Least-cost card acceptance



Collections, categorized and reconciled

Taxes, fees, fines, permits and more are each categorized by type and merchant category and reconciled against the payout rail, so every bank line ties back to a record.

Settlement, balances and holds

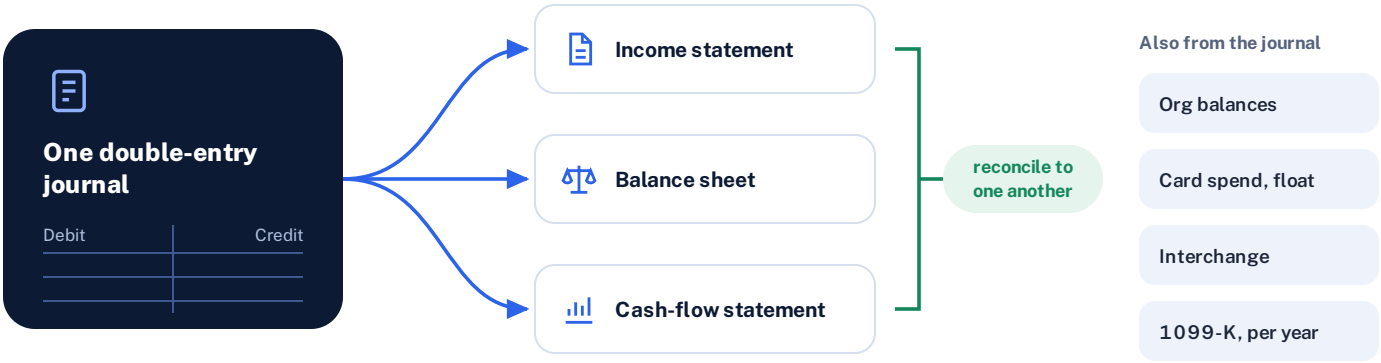
A real settlement engine computes available balance, maturity holds and per-item reserves; only money actually collected is payable, and scoped holds require a different administrator to release.

Issued cards and controlled spend

A card program is provisioned from the same verification, topped up from available balance, with spend categorized by merchant category and interchange and float reported on the console.

One console. One set of books.

Every report comes from the same journal that records every transaction, so there is no separate, divergent reporting system to reconcile.



Double-entry platform accounting

A single double-entry journal produces an income statement, a balance sheet and a cash-flow statement that reconcile to one another, so the financial picture is always internally consistent and auditable.

Reporting that ties to the record

Per-organization balances, card spend, interchange and float, and 1099-K readiness per year are produced from the same journal that records every transaction.

Included and live from day one

- Card acceptance, online and in person
- Double-entry accounting and 1099-K readiness
- AES-256 encryption, MFA and audit trail
- Least-cost routing and Level 2/3 interchange
- Balances, holds, reserves and payouts
- OFAC screening and the data-governance wall
- Self-hosted AI, no external data sharing
- Issued-card program with spend reporting

Start with one application.

Identity and business verification are built in. Then run collections, settlement, cards and reporting from one console.

SolutionsAe Financial d/b/a GoodForUs
srv1974040.hstgr.cloud