CAPCHACLOUD

Current Platform Proposal & Vendor Due-Diligence Package

CapchaCloud identity, consent, signing, screening, transaction evidence and Chargeback Armor for VeraBank, N.A.

Confidential — prepared for VeraBank, N.A. vendor evaluation. Not for further distribution without CapchaCloud's consent.

EVIDENCE Tamper-evident records	OVERLAY Non-blocking, additive	VERIFIABLE By any third party, offline

Prepared for	VeraBank, N.A. — Compliance / Vendor Risk Review
Prepared by	CapchaCloud (a ServiceAutomations.ai product)
Date	July 29, 2026
Status	Confidential discussion draft — vendor due-diligence package

Proposal premise: VeraBank keeps its existing channels, controls, decision engines, processor, core and adjudication authority. CapchaCloud adds a separate, non-blocking evidence plane after or alongside each event.

1. Executive summary

CapchaCloud does not ask VeraBank to replace its website, digital banking provider, CRM, account-opening platform, Positive Pay service, fraud models, identity provider, processor or core. VeraBank continues to make every business and risk decision, including dispute adjudication. At an in-scope event, VeraBank can use a widget, make one authenticated API call, call the typed SDK, receive a signed webhook, or use authorized MCP administration. CapchaCloud returns a durable evidence reference that VeraBank stores beside its existing record.

> WRITTEN FOR COMPLIANCE REVIEW
> This package is written for compliance review first. It states plainly what CapchaCloud is certified for and what it is not, what data it needs and what it is designed never to receive, and how VeraBank's third-party risk obligations map onto the engagement. CapchaCloud's product premise is verifiable honesty — the same posture governs this proposal. Section 10 is a candid register of our known gaps, stated before VeraBank's diligence finds them, each with the compensating control we propose.

This document is organized into fourteen sections: vendor and product information (Sections 2–4), the regulatory, data-governance, security, resilience and third-party-risk sections written specifically for compliance review (Sections 5–10), and architecture, commercial terms, implementation plan and sources (Sections 11–14).

Three headline facts for compliance review

- Data minimization by design: the pilot pattern uses VeraBank-generated pseudonymous references and content hashes. Account numbers, SSNs, card data, credentials and balances are not required and are contractually out of scope.
- Evidence survivability: every sealed record can be exported as a self-contained bundle and verified offline with a published zero-dependency script — the evidentiary value of VeraBank's records does not depend on CapchaCloud's continued existence. This directly addresses vendor-exit risk.
- Non-blocking: default integration is asynchronous and fail-open; a CapchaCloud outage cannot stop a VeraBank customer journey.

2. Vendor profile

Factual vendor identification for the diligence file. No claims beyond what is stated below.

Field	Value
Product	CapchaCloud — proof infrastructure platform (CapchaID, consent evidence, CapchaSign, CapchaVerify, CapchaShield, transaction/ISO 20022 sealing, and dispute evidence automation)
Operator	ServiceAutomations.ai
Principal contact	Adam Woodward, Founder
Infrastructure	100% Cloudflare (Workers, D1, R2, KV, Queues) — no self-operated servers or data centers
Intellectual property	Multiple U.S. provisional patent applications filed (2026) covering the evidence-sealing and verification methods
Public verification surfaces	Live transparency endpoint, public chain explorer, downloadable offline verifiers — available to VeraBank's reviewers today, before any engagement
Corporate/financial detail	Provided directly at the discovery session (entity documents, ownership, financial condition)

CapchaCloud is an early-stage vendor and this package does not pretend otherwise. Section 8 (exit strategy) and Section 10 (gaps register) address the risk questions that fact properly raises.

3. Services description

Independent of Chargeback Armor (Section 4), CapchaCloud's capabilities are available individually as a per-use-case services menu. Every action is metered in a single credit currency, so VeraBank can adopt one service, several or all of them without a separate contract for each.

Service	What it does	Where it fits at VeraBank	Unit price
Consent & disclosure evidence	Seals the exact disclosure or authorization language presented, together with origin and available identity/device context	Marketing consent (TCPA), e-sign consent, account disclosures, treasury agreements	6 credits (≈$0.03) per certificate
CapchaSign e-signature	Envelope lifecycle with templates, fields, sequential signing, identity tiers, optional pay-at-signing/video consent, sealed output and public verification	Loan documents, account agreements, treasury onboarding	100 credits (≈$0.50) per completed envelope
CapchaID authentication	Social OAuth, email/password, magic link, email OTP, TOTP 2FA, sessions and JWKS/JWT, with auth evidence linked to the proof chain	Employee, customer or merchant authentication and session disputes	1 credit (≈$0.005) per session
ISO 20022 message sealing	Seals pacs.008 etc. into tamper-evident evidence; UETR-scoped corroboration when the pacs.002/.004 comes back	Wire evidence, FedNow readiness, payment-investigation files	10 credits (≈$0.05) per message
Native screening (CapchaVerify)	Sanctions-list screen, device signals, transaction monitoring — native, no vendor license. Explicitly NOT certified KYC	Pre-screen before certified checks; ongoing monitoring evidence	10 credits (≈$0.05) per screen; media checks 30 credits (≈$0.15)
Certified KYC orchestration (CapchaShield)	Runs checks through VeraBank's OWN contracted vendor (Sumsub/Jumio/etc. — bring-your-own credentials), seals the outcome as evidence; vendor bills VeraBank directly	Account opening, CIP files, case management	70 credits (≈$0.35) per orchestrated check + vendor's own fee
Dispute / defense packets	Matches a dispute to a sealed record and generates a human-readable and machine-readable evidence package for an authorized case owner	Reg E files, chargeback representment preparation, counsel review	Included with sealed records
Public verification	Anyone — auditor, examiner, opposing counsel — can verify a record's integrity with no login and no PII exposure; offline verifier scripts published	Vendor-risk review, examiner requests	Free, public

Note: every action above is metered in one credit currency on one bill. Plan tiers range from $0/month (500 credits) to Enterprise plans from $999/month (250,000+ credits, with volume discounts at scale). Credits are sold in prepaid packs that never expire; there is no metered surprise overage.

Agent-native operations

CapchaCloud also exposes an authenticated remote MCP (Model Context Protocol) control surface for machine-to-machine administration. Current public integration materials describe tenant provisioning, branding, sites, exports, SSO/SCIM configuration, ConsentWallet, ISO 20022, CapchaShield and audit-chain operations. The proposal intentionally does not quote a fixed tool count because the control surface changes as the platform ships.

4. Chargeback Armor: evidence generated and routed when a transaction is disputed

Chargeback Armor closes the loop between transaction-time evidence and dispute operations. Every covered transaction receives a durable record reference. When VeraBank or its processor reports a dispute, Armor correlates the case to that record, assembles a reason-code-aware package and routes it to the authorized case owner. VeraBank, the merchant, its processor or counsel performs any network, Nacha, court or regulatory submission.

THE OPERATING MODEL
Transaction record in -> dispute event received -> evidence matched -> packet generated -> authorized owner reviews/submits -> outcome recorded. VeraBank keeps its processor, card platform, case system and adjudication authority.

Automated dispute workflow

Stage	Input	Chargeback Armor action	Output
1. Seal	Processor transaction reference, terms, authentication and fulfillment evidence	Create tamper-evident record and return record_id	Record ID stored beside VeraBank transaction
2. Detect	Dispute-opened webhook or case feed with case ID, reason code and deadline	Match transaction and validate tenant/merchant ownership	Matched case or exception queue
3. Assemble	Sealed record plus permitted supporting artifacts	Select evidence relevant to the reason code and create packet manifest	Human-readable packet plus machine-readable evidence
4. Route	Authorized VeraBank, merchant, processor or counsel destination	Deliver by API, signed webhook or structured export; retry transient delivery failures	Submission-ready packet, timestamp, packet hash and delivery acknowledgment
5. Record	Outcome supplied by the authorized case owner or processor feed	Attach the outcome to the evidence trail when provided	Portfolio reporting and audit trail

Two distinct VeraBank opportunities

Lane	What is disputed	Chargeback Armor role
Issuer-side debit disputes	A VeraBank customer disputes a debit-card transaction through digital banking or customer service.	Attach the sealed transaction and authentication record to VeraBank's investigation/network case. Armor does not override Regulation E or VeraBank's adjudication.
Merchant-services chargebacks	A cardholder at another issuing bank disputes a transaction accepted by a VeraBank merchant-services customer.	Create the representment evidence packet; the merchant, VeraBank or its processor performs the authorized submission.

Corrected VeraBank scale

VeraBank publicly reports one bank with 42 branches, 550+ employees and $4.4 billion in assets - not 42 or 43 separate banks. Dispute volume should be modeled from active cards, merchants and transactions rather than branch count. Five thousand annual disputes would equal only 417 per month across the company, so it is too low to serve as the central combined issuer-plus-merchant scenario.

Illustrative active debit cards	Transactions/card/month	Annual transactions	Disputes at 0.05%-0.20%
50,000	25	15 million	7,500-30,000
100,000	25	30 million	15,000-60,000
150,000	25	45 million	22,500-90,000

Issuer-side sensitivity only. VeraBank does not publicly disclose active debit cards, transaction volume or dispute rate; every input above is an assumption for discovery.

Illustrative merchants	Transactions/merchant/month	Annual transactions	Chargebacks at 0.15%-0.40%
500	1,500	9 million	13,500-36,000
1,500	1,500	27 million	40,500-108,000
3,000	1,500	54 million	81,000-216,000

Merchant-side sensitivity only. The underlying processor may handle many cases without VeraBank staff involvement; discovery must obtain total processor disputes, not only internal escalations.

Recommended planning range and value illustration

Until VeraBank supplies portfolio data, use 20,000 annual disputes as a low case, 50,000-100,000 as the central planning range, and 150,000+ as a high-volume sensitivity. At a 75,000-dispute midpoint, saving 15 minutes per case at $35 per loaded labor hour produces $656,250 in annual labor value. An additional $20 recovered per dispute adds $1.5 million, for approximately $2.16 million of illustrative annual value before platform, integration and vendor-management costs.

Pilot measure	Target	Proof
Disputes matched automatically	70-90%	Processor case ID linked to the correct sealed transaction
Complete packets ready before deadline	>=99%	Packet-ready timestamp before the applicable deadline
Manual evidence-assembly time	50-80% lower	Timed baseline vs. automated packet sample
Evidence completeness	>=95%	Reason-code checklist present before release
Incorrect record matches	<1%	Case audit comparing the dispute and sealed transaction

LAST-MILE REQUIREMENT
CapchaCloud assembles, verifies and routes evidence. It does not submit directly to Visa, Mastercard, Nacha, a court or a regulator. Final submission remains with VeraBank, the merchant, its processor or counsel, including where a provider exposes only a portal.

5. Regulatory mapping

CapchaCloud provides recordkeeping and evidence infrastructure. It does not provide legal advice, does not adjudicate disputes, and does not replace any VeraBank compliance obligation. The table below maps where sealed evidence supports VeraBank's existing obligations.

Regulation / framework	VeraBank's obligation (summary)	How CapchaCloud evidence supports it	What CapchaCloud does NOT do
E-SIGN Act / UETA	Electronic signatures and records valid when consent and attribution requirements are met	CapchaSign captures signer consent-to-e-sign, attribution evidence, identity-assurance tier, document/field state and a sealed completion certificate with public verification	Does not opine on enforceability of any specific instrument
Regulation E (12 CFR Part 1005) error resolution	Investigate alleged errors within required timeframes; document findings	Chargeback Armor assembles the sealed transaction, authentication and consent evidence for the investigation file and records delivery/outcomes when provided	Does not decide claims; adjudication and all Reg E determinations remain entirely VeraBank's
Card-network dispute rules (merchant services)	Representment evidence per network reason codes and deadlines	Reason-code-aware packet assembly from sealed transaction-time evidence, routed to VeraBank, the merchant or its processor	Does not submit directly to Visa, Mastercard, Nacha or another network
TCPA / FTC Telemarketing Sales Rule	Prior express written consent where required; TSR record retention (5 years)	Consent certificates seal the exact disclosure presented, identity fields, origin forensics, and a dual bot-screen verdict; 5-year retention floor, billing-independent	Does not determine which consent standard applies to a given campaign
FRE 902(11)/(13)/(14) (evidence posture)	Records of regularly conducted activity; records generated by an electronic process; data authenticated by hash verification	Defense packets and evidence bundles are structured to support self-authentication workflows, including hash-verification affidavit support (902(14))	Admissibility is always the court's determination; CapchaCloud supplies the verifiable record, not the ruling
GLBA Safeguards (vendor dimension)	Oversee service providers; appropriate safeguards for customer information	Pilot design keeps NPI out of scope entirely via pseudonymous references; where production scope later includes NPI categories, encryption, access controls, and retention locks apply	Not a substitute for VeraBank's information-security program
BSA/AML	CIP/KYC, screening, monitoring per VeraBank's program	CapchaShield orchestrates checks through VeraBank's OWN contracted vendors and seals outcomes as evidence; CapchaVerify native screens are explicitly not certified KYC and are labeled as such in-product	CapchaCloud is not a BSA program component and does not perform certified identity verification itself
Interagency Third-Party Relationships guidance (2023)	Risk-based lifecycle management of third parties	Section 9 of this document maps the full lifecycle; CapchaCloud commits to due-diligence support, contractual audit rights, and termination/export provisions	—

6. Data governance & data flows

What CapchaCloud receives

Three integration patterns govern what reaches CapchaCloud: asynchronous API calls made after VeraBank has already accepted or created an event; synchronous API calls made before workflow routing; and a browser widget used at a public form or consent moment. Section 11 (Integration modes) describes the customer-impact and recommended use of each pattern in full.

- Pilot data rule: use VeraBank-generated pseudonymous event and party references; the mapping stays inside VeraBank. The sample payload in Section 11 intentionally omits account number, SSN, credentials, balances, and payment-card data.
- What never leaves CapchaCloud to external anchors: only cryptographic hashes are sent to the RFC-3161 timestamp authority and OpenTimestamps/Bitcoin calendar servers — no record content, no PII, no VeraBank identifiers.

Storage & encryption

Evidence objects are held in retention-locked (WORM) object storage with provider-managed AES-256 encryption at rest; TLS protects data in transit. Metadata is held in a relational store. Primary storage is in U.S. Cloudflare regions (current production primary: United States; residency constraints should be confirmed at discovery). Processing occurs at the Cloudflare global edge.

Retention

A five-year retention floor applies and is independent of billing status. Legal holds extend retention indefinitely. Retention is enforced by the storage layer through compliance retention locks, not by application logic alone.

Subprocessors

Subprocessor	Role	Data scope
Cloudflare	Infrastructure, storage and compute	All hosted evidence data and metadata
Stripe	Billing only	No evidence data; payment and subscription information only
Transactional email provider	Delivery of invites and notices	Recipient email address and message content of the notice itself
RFC-3161 timestamp authority + OpenTimestamps calendars	Independent timestamp anchoring	Cryptographic hashes only

Full subprocessor list with roles is provided at contracting; subprocessor changes are subject to notice.

Data subject / consumer surface

Public verification endpoints return integrity status without PII. Consumer-facing wallet, export and revocation-request surfaces exist for consent records.

7. Information security program

Encryption: TLS in transit (Cloudflare edge), AES-256 at rest (object storage), API credentials stored hashed; secrets in the platform secret store, never in code or client assets.

Tamper evidence: Append-only hash-chained audit log (fork-proof CAS design), records folded into Ed25519-signed Merkle blocks, dual-anchored (RFC-3161 TSA + Bitcoin via OpenTimestamps), public transparency endpoint, public chain explorer, downloadable zero-dependency offline verifiers.

Software assurance: 1,400+ automated tests, CI-gated releases, CI-gated OpenAPI contract, automated dependency monitoring (Dependabot) with report-only vulnerability audit in CI, scheduled production end-to-end smoke checks, top-level error-boundary alerting.

Access control: Role-based tenant model; operator (superadmin) access restricted by allowlist; per-tenant API keys hashed at rest, rotatable; rate limiting on every write route (atomic, Durable-Object-backed) with per-tenant caps.

Security posture: Public materials describe TLS 1.2+, HSTS, encrypted Cloudflare storage, hashed API keys, HMAC-signed webhooks, replay controls, incident response and a published trust surface. VeraBank should verify each control and request supporting evidence during diligence.

Vulnerability disclosure: Security contact published; issues acknowledged and tracked to remediation.

Stated plainly: CapchaCloud's public materials do not provide a SOC 2 report or certification, and do not cite an independent third-party penetration-test report. VeraBank should require current evidence during diligence rather than treating roadmap language as certification. See Section 10 for the full gaps register and proposed compensating controls.

8. Business continuity, resilience & exit strategy

Platform resilience: All services run on Cloudflare's global anycast network (300+ points of presence); no single self-operated server exists in the architecture.

Backup/recovery: Point-in-time recovery on the metadata store (30-day window); object storage designed for eleven-nines durability; queue-based webhook delivery with retry and dead-letter capture.

Availability transparency: Public status page with uptime history and incident log; proposed pilot availability target 99.9% monthly for API endpoints (formal SLA at production contracting).

Fail-open default: Integration is asynchronous; an outage degrades evidence capture into a VeraBank-controlled retry queue, never a blocked customer.

Exit strategy

EXIT STRATEGY — LEAD WITH THIS
Sealed records can be exported with integrity material for independent verification. Public certificates, the chain explorer and offline verification reduce dependency on the CapchaCloud dashboard. Contracting should define complete export, retention and transition assistance so VeraBank can preserve already-sealed evidence if the relationship ends.

9. Third-party risk management alignment

This section maps the engagement onto the interagency third-party relationship risk-management lifecycle.

Lifecycle stage	What VeraBank needs	What CapchaCloud provides
Planning	Risk assessment of the proposed relationship	This document; pilot scoped to non-NPI pseudonymous data; fail-open architecture
Due diligence	Vendor evaluation evidence	Security questionnaire support; live public transparency/verification surfaces reviewable today; entity/financial documents at discovery; references as the customer base matures (stated honestly)
Contracting	Enforceable protections	Audit rights; data-scope schedule (what may and may not be transmitted); SLA; breach notification; termination/export provisions; subprocessor notice
Ongoing monitoring	Continuing oversight	Public status page + uptime history; live transparency endpoint; quarterly service reviews; incident notification commitments
Termination	Orderly exit	Full evidence export; offline verifiability independent of vendor; retention survivability

CapchaCloud enters production only after VeraBank's risk, legal, information-security, and privacy teams approve the intended data flow.

10. Known gaps & compensating controls

This is a candid register of CapchaCloud's known gaps as of the date of this proposal, stated before VeraBank's diligence finds them.

Gap	Status stated plainly	Compensating control / roadmap
SOC 2 examination	No report or certification is provided in current public materials; the roadmap describes an engagement as planned	Pilot scoped to pseudonymous, non-NPI data; VeraBank obtains direct evidence and contract commitments before production
Independent penetration test	No independent report is cited in current public materials	Require current test scope, remediation evidence and retest results during diligence; keep pilot non-sensitive and shadow-mode
CapchaSign legal posture	Sealed records strengthen attribution and integrity but do not guarantee enforceability	VeraBank and counsel approve the document classes, consent language, identity tier and retention policy
Operating history	Early-stage vendor; limited production track record and reference base	Exit-strategy design (Section 8): evidence remains verifiable without the vendor; month-to-month terms; no lock-in
Insurance	E&O/cyber coverage not yet bound; procurement planned before production go-live	Pilot carries no NPI and is fail-open; coverage certificates provided at production contracting
Team depth	Small team; key-person concentration	Fully managed infrastructure (no servers to maintain), infrastructure-as-code, documented runbooks, and the evidence survivability guarantee above

WHY DISCLOSE THIS HERE
We would rather VeraBank read this table here than discover it in diligence. Every row has a date-able roadmap item, and pilot scope is designed so that none of these gaps exposes VeraBank data or operations while they close.

11. Architecture & integration

A separate evidence plane, not a replacement platform

The deployment pattern is intentionally additive. VeraBank retains the customer journey, source systems, risk engines and final decisions. CapchaCloud receives only the minimum event material needed to create or verify evidence.

1 Customer channel Existing VeraBank site, app or operator	2 Existing workflow Form, login, decision or payment instruction	3 One API call Signed, idempotent, minimal payload	4 Evidence plane Screen, hash, timestamp, chain and store	5 Existing record Store record ID in CRM, core or case tool

Logical architecture. CapchaCloud is not in the funds path and does not execute, approve, block, reverse or settle transactions.

Integration modes

Mode	Where it fits	Customer impact	Recommended use
Widget	At authentication, public form or consent moments	Small client integration	CapchaID and supported consent/proof flows
API + typed SDK	From VeraBank services and workflow engines	Network call only	Transaction, signing, screening and ISO 20022 evidence
Signed webhooks	Back into VeraBank systems	None	HMAC-SHA256 delivery, logs, replay and downstream case updates
Remote MCP	Authorized operator and automation workflows	None	Tenant administration, configuration, exports and audit operations

Technical integration: one call, one receipt

CapchaCloud publishes an OpenAPI 3.1 contract. Authenticated write endpoints accept a Bearer token or X-API-Key. Write calls support an Idempotency-Key header with a 24-hour replay window, allowing VeraBank to retry without intentionally creating duplicate records.

Illustrative transaction-evidence call

```
POST https://capchacloud.com/api/v1/txn/seal
Authorization: Bearer ${CAPCHACLOUD_API_KEY}
Idempotency-Key: verabank:event:8d2c1f...
Content-Type: application/json

{
  "rail": "internal",
  "rail_ref": "vb_evt_8d2c1f...",
  "terms": "Exact authorization language presented by VeraBank",
  "include_terms": false,
  "parties": [
    {
      "role": "customer",
      "human_verified": true,
      "identity_assurance_level": "authenticated"
    }
  ]
}
```

CapchaCloud seals the event and returns the API result defined by the OpenAPI contract. VeraBank stores the returned record reference alongside vb_evt_8d2c1f.... Public verification endpoints can later confirm integrity without returning PII. The example intentionally omits account number, SSN, credentials, balances and payment-card data.

Core API surface relevant to VeraBank

Endpoint	Purpose	Suggested bank use
CapchaID auth + JWKS routes	OAuth, email/password, magic link, OTP, TOTP 2FA, sessions and JWT verification material	Employee, customer or merchant authentication
POST /api/v1/verify-lead	Email/phone quality, suppression and consent-oriented checks	Public business-banking or treasury inquiries
POST /api/v1/txn/seal	Seal terms, parties and a pseudonymous rail reference	Authorization, exception or operational-decision receipt
POST /api/v1/iso20022/seal	Seal exact ISO 20022 bytes in vaulted or hash-only mode	Payment-message evidence outside the payment rail
CapchaSign envelope routes	Create, send, sign and complete envelopes with fields and identity tiers	Internal or customer document workflows
CapchaShield case/evidence routes	Run BYO-vendor checks, manage cases and export evidence packages	KYC/AML program evidence and examiner files
POST /api/v1/defense-packet	Create an evidence memo for a record	Case handling, counsel review and complaint response

Operational behavior

- Default pilot behavior is non-blocking: if CapchaCloud is unavailable, VeraBank's workflow continues and the event enters a VeraBank-controlled retry queue.
- For evidence-mandatory workflows, VeraBank may choose a hold-for-review policy; CapchaCloud does not impose that policy.
- Webhook events are HMAC-SHA256 signed and can be replayed from the delivery log.
- Origin allowlists, per-tenant API keys and separate sandbox credentials constrain the integration boundary.
- Secrets remain in VeraBank's secret manager and must never be placed in browser code or logs.

12. Proposed 60-day pilot and commercial terms

The pilot is designed to prove incremental value with minimal operational risk. Scope starts with a channel that does not collect sensitive banking information, run in shadow mode.

Pilot scope - select one or two lanes

- (a) Chargeback Armor in shadow mode on one dispute feed - issuer-side debit disputes, or one merchant-services portfolio.
- (b) Consent/disclosure evidence on one public business-banking intake form.
- (c) CapchaSign on one internal or low-risk document flow.

Phase	Timing	Work	Exit gate
1. Due diligence	Days 1-10	Data map, DPA, subprocessor review, security evidence, retention decision and success-metric baseline	Written approval for sandbox/shadow scope
2. Integration	Days 11-20	Create sandbox tenant, allowlist domain, add widget or API call, register webhook and instrument metrics	End-to-end test with synthetic records
3. Shadow mode	Days 21-35	Score and seal events without changing customer routing; compare output to existing outcomes	False-positive and latency thresholds met
4. Limited live	Days 36-55	Enable routing or challenge policy for a controlled percentage of traffic	No material CX or operational regression
5. Decision	Days 56-60	Measure abuse reduction, evidence coverage, labor savings, incidents and total cost	Scale, revise or remove with documented rationale

Pilot scorecard

- Quality baseline vs. pilot: accepted abuse and downstream outcomes before and during the pilot.
- Verified bot outcomes: automated/abusive submissions correctly identified and stopped.
- Downstream rejection rate: legitimate submissions incorrectly challenged or rejected.
- Dispute match rate: share of disputes automatically matched to a sealed transaction record.
- Packet turnaround time: elapsed time from dispute event to a complete packet ready for authorized review/submission.

Commercial terms

Item	Terms
60-day pilot	$4,900 flat. Includes up to 100,000 sealed events, integration support, and a named success scorecard agreed before start.
Production	Enterprise plan from $999/month (250,000 credits included), plus credit usage per the services menu (Section 3). Volume discounts at scale.
No lock-in	Cancel anytime. Evidence already sealed remains verifiable and exportable; the five-year retention floor survives cancellation.
No surprise billing	No metered overage. Prepaid credit packs only, never expiring.
Contract provisions	Audit rights, breach notification, data-scope schedule, subprocessor notice, termination/export — all included in the pilot agreement.
Availability	99.9% monthly API availability target during pilot; formal SLA at production contracting.

13. Implementation plan & next step

The implementation plan below sequences the discovery, sandbox-integration and shadow-mode work already scoped in Section 12 into a compliance-reviewable timeline.

Timing	Milestone	Work
Week 0	Discovery & vendor-risk session (compliance, infosec, ops)	Select workflow(s); agree data-scope schedule and pseudonymization convention; baseline metrics. No production banking data required.
Weeks 1–2	Sandbox integration	VeraBank test tenant; sample payloads; verification walkthrough with VeraBank's own reviewers running the offline verifier.
Weeks 3–8	Shadow-mode pilot	Sealed evidence runs parallel to existing operations; weekly metrics against the agreed scorecard.
Week 9	Scorecard review	Go/no-go on production contracting with full legal/vendor-risk terms.

DECISION REQUESTED
Authorize the Week-0 discovery session to select one workflow, establish baseline metrics, and determine whether a sandbox pilot is appropriate. No production banking data is required for that decision.

14. Sources and method

External statistics are included to establish market context. CapchaCloud-specific capabilities are drawn from its published product, OpenAPI, trust and evidence materials. The fraud-reduction percentages in this proposal are explicitly labeled pilot targets or sensitivity assumptions.

1. Federal Trade Commission. FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025. Accessed July 29, 2026. https://www.ftc.gov/news-events/news/press-releases/2026/06/ftc-data-show-people-reported-losing-3-point-5-billion-imposter-scams-2025

2. Federal Bureau of Investigation. 2025 IC3 Annual Report. Accessed July 29, 2026. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

3. Association for Financial Professionals. 2025 Payments Fraud and Control Survey press release. Accessed July 29, 2026. https://www.afponline.org/about/learn-more/press-releases/Details/survey-79-percent-of-organizations-were-victims-of-attempted-or-actual-payments-fraud-activity-in-2024

4. Federal Reserve Financial Services. 2024 Financial Institution Risk Officer Survey - Key Findings. Accessed July 29, 2026. https://www.frbservices.org/binaries/content/assets/crsocms/news/research/2024-risk-officer-survey-results.pdf

5. VeraBank. Positive Pay. Accessed July 29, 2026. https://www.verabank.com/Business/Banking-Services/Positive-Pay

6. VeraBank. Fraud alerts and controls. Accessed July 29, 2026. https://www.verabank.com/Resources/Security/Fraud

7. VeraBank. Company profile: 42 branches, 550+ employees and $4.4 billion in assets. Accessed July 29, 2026. https://www.verabank.com/Resources/Education-Learning/News-Articles/News/verabank-expands-central-texas-presence-with-opening-of-full-service-branch-in-avery-ranch

8. VeraBank. Merchant Services. Accessed July 29, 2026. https://www.verabank.com/Business/Banking-Services/Merchant-Services

9. VeraBank. Online Banking: debit-card disputes. Accessed July 29, 2026. https://www.verabank.com/Personal/Banking-Services/Online-Banking

10. VeraBank. What are Chargebacks and How to Minimize Them. Accessed July 29, 2026. https://www.verabank.com/Resources/Education-Learning/News-Articles/Resources/what-are-chargebacks-and-how-to-minimize-them

11. CapchaCloud. Current product overview. Accessed July 29, 2026. https://capchacloud.com/

12. CapchaCloud. OpenAPI specification. Accessed July 29, 2026. https://capchacloud.com/openapi.json

13. CapchaCloud. Integration guide. Accessed July 29, 2026. https://capchacloud.com/integrate.md

14. CapchaCloud. Published product facts. Accessed July 29, 2026. https://capchacloud.com/FACTS.md

15. CapchaCloud. Pricing and unified credits. Accessed July 29, 2026. https://capchacloud.com/pricing.html

16. CapchaCloud. Product changelog. Accessed July 29, 2026. https://capchacloud.com/changelog.html

17. CapchaCloud. Roadmap. Accessed July 29, 2026. https://capchacloud.com/roadmap.html

18. CapchaCloud. CapchaVerify. Accessed July 29, 2026. https://capchacloud.com/capcha-verify.html

19. CapchaCloud. CapchaShield. Accessed July 29, 2026. https://capchacloud.com/capcha-shield.html

20. CapchaCloud. CapchaBanking. Accessed July 29, 2026. https://capchacloud.com/capcha-banking.html

21. CapchaCloud. Trust Center. Accessed July 29, 2026. https://capchacloud.com/trust-center.html

22. CapchaCloud. Data Processing Addendum. Accessed July 29, 2026. https://capchacloud.com/dpa.html

23. Office of the Comptroller of the Currency. OCC Bulletin 2023-17: Interagency Guidance on Third-Party Relationships. Accessed July 29, 2026. https://www.occ.treas.gov/news-issuances/bulletins/2023/bulletin-2023-17.html

Important limitations

- CapchaCloud is evidence-oriented infrastructure; it does not guarantee legal, regulatory or fraud outcomes.
- Industry statistics do not estimate VeraBank's fraud exposure or loss experience.
- Modeled savings exclude implementation, vendor-management, security-review and internal change-management costs.
- Production use is subject to VeraBank's due diligence, legal review, data-governance requirements and contract terms.
- This proposal is technical and commercial information, not legal advice.