

■ **FIDUCIARY CHECK**

Built on the regulatory record

Recordkeeping & Archiving Service

Policies & Procedures

Website Content Capture, Retention, and Production for Investment Advisor Clients

Fiduciary Check LLC (Arizona)

Prepared for: Vendor due diligence review

Document version: 1.0 · Effective date: June 30, 2026

Owner: Isac, Operations Lead

Review cycle: Annual, or upon material regulatory change

About this document

This document describes the operational policies and procedures Fiduciary Check LLC follows when capturing and retaining content published on a client's website. It is provided so that an investment advisor's Chief Compliance Officer can evaluate Fiduciary Check as a service provider and place this record in the firm's vendor due diligence file.

It is not legal advice and is not the advisor's compliance program. The advisor remains solely responsible for its obligations under the Investment Advisers Act of 1940 and the rules thereunder. Fiduciary Check recommends the advisor's CCO and/or counsel review this document before relying on it.

1 Purpose and Scope

Fiduciary Check LLC designs, builds, and maintains websites for investment advisory firms. As part of the Turnkey and Compliance Guardian tiers, Fiduciary Check operates a recordkeeping and archiving service that captures and preserves the content an advisor publishes through its Fiduciary Check website.

The purpose of this service is to help an advisor preserve copies of its website-based communications in a form that supports the recordkeeping obligations applicable to advertisements and marketing communications, and to make those records retrievable on demand.

What this service covers

- Public-facing pages of the advisor's website (home, services, about, team, disclosures, and similar pages).
- Blog posts and articles published through the website's admin center, including drafts, edits, and removals.
- Disclosures and disclaimers displayed on the website, including changes to their wording and placement.
- Third-party reviews and testimonials as displayed on the advisor's website (for example, Google reviews republished on a site page), captured as displayed, when displayed.
- Landing pages built for the advisor, where applicable.

What this service does NOT cover

Fiduciary Check captures website content only. The following are outside the scope of this service and require separate arrangements or tools:

- **Email and email newsletters** (including mass marketing emails sent off-platform).
- **Native social media content** on platforms such as LinkedIn, Facebook, X, Instagram, or YouTube, including posts, comments, likes, and direct messages.
- **Text/SMS, chat, and messaging-app communications.**
- **Reviews on third-party platforms themselves** (e.g., the Google or Yelp listing). Fiduciary Check captures only what is displayed on the advisor's website.

Fiduciary Check can integrate a dedicated communications archiver for email or social channels as a separate consulting engagement; that integration is out of scope of the website recordkeeping service described here.

Important boundary

Because this service is website-only, a Fiduciary Check archive is not, by itself, a complete books-and-records solution. An advisor that markets through email or social media must maintain separate archiving for those channels.

2 Roles and Responsibility

Compliance with the securities laws is the advisor's responsibility and cannot be delegated to a service provider. The table below states clearly which party is responsible for what.

Function	Advisor (Client)	Fiduciary Check (Vendor)
Determining what is an advertisement and whether content is fair and balanced	Responsible	Not responsible
Approving content before publication	Responsible (CCO / designee)	Provides workflow tooling only
Required disclosures, testimonial/endorsement disclosures, performance presentation	Responsible	Provides templates / placement; does not adjudicate adequacy
Capturing and retaining published website content	Oversees vendor	Responsible (operates the archive)
Producing records to an examiner on request	Responsible (responds to regulator)	Supports self-service export plus assisted production
Maintaining the firm's written compliance program and CCO function	Responsible (Rule 206(4)-7)	Not responsible

3 Regulatory Framework We Support

Fiduciary Check designs its recordkeeping service around the obligations that apply to a registered investment advisor's marketing communications, and, for dual-registered (hybrid) firms, the broker-dealer recordkeeping rules. The service is intended to support, not satisfy on the advisor's behalf, the following:

Authority	Common name	Relevance to this service
Advisers Act Rule 204-2	Books and Records Rule	Requires advisors to keep copies of advertisements they disseminate, retained at least five years from the end of the fiscal year of last use, the first two years in an easily accessible place. Our snapshot archive and audit log support this.
Advisers Act Rule 206(4)-1	Marketing Rule	Governs advisor advertisements, including testimonials, endorsements, third-party ratings, and performance. We capture how content and its disclosures appeared as published; the advisor remains responsible for substance.
Advisers Act Rule 206(4)-7	Compliance Rule	Requires the advisor to adopt written policies and procedures and designate a CCO. This is the advisor's obligation; our service is a tool the program may rely on.
Regulation S-P	Privacy / Safeguards	Governs protection of nonpublic personal information and oversight of service providers. Addressed in Section 9.
Exchange Act Rule 17a-4	BD records [DUAL]	For dual-registered firms: requires WORM or the audit-trail alternative, dual-format production, and redundancy. Our S3 Object Lock store (WORM) and hash-chained audit log (audit-trail) are built to meet both.
FINRA Rules 4511 & 2210	BD records / comms [DUAL]	For dual-registered firms: books-and-records preservation and principal pre-approval of retail communications. Our review workflow records the approving principal and date.

Retention periods

RIA advertisements (204-2): 5 years from end of fiscal year of last use; first 2 years easily accessible. Broker-dealer communications (17a-4 / FINRA 2210): 3 years. For dual-registered firms, Fiduciary Check applies the longer 5-year period uniformly. The system default retention is 5 years, configurable upward on request.

4 How Content Is Captured

System and data flow

Client sites are built in React (Next.js) and hosted on Vercel. When a page, blog post, article, or disclosure is published or changed in the admin center, the system places a job on a queue (AWS SQS) that triggers a capture worker (Playwright on AWS compute). The worker renders the published content, writes the snapshot bundle to immutable storage (Amazon S3 Glacier Instant

Retrieval with Object Lock), and writes a corresponding entry to the append-only audit log (Supabase / PostgreSQL).

Point-in-time snapshots

Each snapshot is a rendered, point-in-time copy of the content as it appeared to the public, captured on every publish or edit. Each snapshot bundle includes rendered HTML, a full-page PDF and PNG (human-readable), the underlying source, and metadata (URL, tenant, timestamp, version, and a SHA-256 content hash). Snapshots are the primary record and are designed to answer the question an examiner is most likely to ask: show me what this page looked like on this date.

Change log (audit trail)

Each change is recorded as a permanent, append-only entry capturing the item, the action (create, edit, publish, unpublish, delete, capture, approve), the date and time, the user identity, the version, the snapshot reference, and a hash chained to the prior entry so that any alteration of the log is detectable. The change log supplements the snapshot archive; it does not replace it.

Removed and unpublished content

When content is unpublished or deleted from the live site, its snapshots and log entries are retained for the full retention period. Removal from the public site does not remove the record from the archive.

5 Retention, Accessibility, and Production

Parameter	Standard applied
Minimum retention	5 years from the end of the fiscal year of last use (default). Configurable to a longer period on request.
Immutability	Amazon S3 Object Lock in Compliance mode: records cannot be altered or deleted by any user, including the account root, before retention expires.
Ready accessibility	All records remain immediately retrievable for the full retention window (Glacier Instant Retrieval returns in milliseconds).
Self-service production	The firm can download its own records (snapshots and audit log) on demand from the admin center at any time.
Assisted production	For bulk examination packages, Fiduciary Check provides an assembled export within 48 hours of request.
Export formats	PDF and PNG (human-readable) plus CSV and JSON (machine-readable / reasonably usable electronic format), with an integrity-verification report.
Retention after removal	Continues for the full period after content is unpublished or deleted from the live site.

6 Integrity, Security, and Access Controls

- **Immutable storage.** Snapshots are written to S3 Object Lock (Compliance mode), providing non-rewriteable, non-erasable (WORM) retention.
- **Tamper-evident audit trail.** Audit-log entries are append-only and hash-chained; any modification breaks the chain and is detectable.
- **Encryption.** Data is encrypted in transit (TLS) and at rest using keys managed in AWS KMS.

- **Access control.** Access is restricted to authorized users, scoped per client (tenant isolation), and itself logged. Advisor personnel access only their own firm's records.
- **Redundancy.** The archive is replicated to a second AWS region (see Section 9), satisfying the redundancy expectation for dual-registered firms.

Operational logs vs. the compliance record. *System telemetry (error tracking and uptime monitoring via Sentry; infrastructure logs in AWS CloudWatch) is kept short-retention for operational purposes and is separate from the compliance record. The books-and-records are the snapshots (S3) and the audit log (PostgreSQL), retained for the full period.*

Note: *Advisers Act Rule 204-2 requires electronic records be protected from alteration, loss, or destruction with controlled access. S3 Object Lock Compliance mode also satisfies the WORM option under Exchange Act Rule 17a-4 for dual-registered firms.*

7 Testimonials and Third-Party Reviews

Reviews and testimonials displayed on an advisor's website (including Google reviews republished on a site page) are treated as advertisements under the Marketing Rule and are captured by Fiduciary Check as displayed, when displayed, with the same snapshot-and-log treatment as other content.

Division of responsibility for reviews

Fiduciary Check captures and retains what is displayed. The advisor, through its CCO, decides which reviews to display and is responsible for required testimonial and endorsement disclosures, for not presenting reviews in a misleading or cherry-picked manner, and for any adoption or entanglement determinations. Fiduciary Check does not select, edit, or vouch for displayed reviews.

8 Optional Modules

Pre-publication review & approval workflow (Turnkey tier and above)

Content drafted in the admin center can be routed to the advisor's CCO or designee (and, for dual-registered firms, a registered principal) for approval before it goes live. The approval (approver identity, decision, date and time, version approved) is recorded in the audit log, giving the advisor evidence that an advertisement was reviewed prior to dissemination and supporting FINRA Rule 2210 principal pre-approval where applicable. The decision is always the advisor's.

AI Compliance Guardian (Compliance Guardian tier only)

The AI Compliance Guardian screens draft copy against patterns associated with advertising and communication rules and flags wording that may warrant review. It runs on Amazon Bedrock using Anthropic's Claude models. Bedrock does not use prompts or outputs to train models, and data remains within Fiduciary Check's AWS account and region. The Guardian is a first-pass drafting aid; it is not a compliance determination, does not approve content, and does not replace the advisor's review and sign-off. Screening results are logged.

9 Data Handling, Privacy, and Subprocessors

Data residency

All client data is stored in the United States. The primary archive is in AWS US West (Oregon, us-west-2) and is replicated to AWS US East (N. Virginia, us-east-1). The application database and audit log are hosted with Supabase in US East (us-east-1).

Nonpublic personal information (NPI)

The website-archiving service handles public-facing marketing content only, the content the advisor publishes on its site. It does not collect or require client NPI. The Regulation S-P exposure of this service is therefore limited by design.

Subprocessors

The following providers may process data in the course of delivering the service. Self-hosted components (e.g., Playwright, and self-hosted analytics) run within Fiduciary Check's own infrastructure and are not third-party subprocessors.

Provider	Role	Data it touches	Residency
Amazon Web Services	Archive (S3 Glacier IR + Object Lock), compute (capture workers), queue (SQS), key management (KMS), operational logs (CloudWatch), AI screening (Bedrock / Claude)	Published website content; system metadata; screening text. Bedrock does not train on data.	US (us-west-2, us-east-1)
Supabase	Application database, authentication, append-only audit log	Content metadata and audit records	US (us-east-1)
Vercel	Hosting and delivery of client websites	Public website content	US
Cloudflare	DNS, CDN, and WAF for client domains (managed by Fiduciary Check; client owns the registration)	Public DNS and traffic	Global edge
Resend	Transactional / system email (approval notices, alerts)	Recipient addresses; notification content	US
Sentry	Error tracking and uptime monitoring	Operational telemetry (not the compliance record)	US
Stripe	Billing and payment for Fiduciary Check's fees	Fiduciary Check billing data	US

Fiduciary Check maintains this list, conducts due diligence on each subprocessor consistent with current Regulation S-P service-provider-oversight expectations, and will provide updates on request.

Incident response

Fiduciary Check maintains an incident-response process and will notify the affected advisor within 48 hours of confirming a security incident affecting that firm's records, consistent with its agreement and applicable law.

10 Termination, Portability, and Domain Ownership

Domain ownership

The advisor owns its domain registration at all times. Fiduciary Check manages the domain's DNS, CDN, and security through Cloudflare on the advisor's behalf and with its authorization. Fiduciary Check does not take ownership of the advisor's domain.

Termination and data portability

On termination, the advisor may request a complete export of its archive so it can continue to meet its own retention obligations with a successor solution, and DNS control is returned to the advisor. Because records are held under Object Lock in Compliance mode, they remain immutable for the balance of their retention period; Fiduciary Check will not delete an advisor's archive without written instruction and confirmation that the advisor has retained its required records.

11 Document Control

Version	Date	Owner	Summary of change
1.0	June 30, 2026	Operations (Isac)	Initial issue.

Disclaimer

This document describes Fiduciary Check LLC's service and operational procedures. It is provided for vendor due-diligence purposes and is not legal advice. It does not create any representation that use of Fiduciary Check's services renders an advisor compliant with any law or rule. Compliance with the Investment Advisers Act of 1940 and the rules thereunder is the advisor's responsibility. Advisors should consult their own compliance personnel and counsel.