Sum Certain

TRUST BOOKKEEPING FOR LAW FIRMS

Vendor Diligence Packet

Prepared for law firms evaluating Sum Certain LLC as a service provider, and for the accountants and advisors who refer them.

Version 1.1 · July 23, 2026
Reviewed quarterly

getsumcertain.com
hello@getsumcertain.com

HOW TO USE THIS PACKET

Answers, so you don't have to schedule a call

Your firm has an obligation to vet the service providers who touch client information. This packet exists so that vetting can happen from a document in your file rather than a conversation on your calendar.

It is organized around the four ABA Formal Opinions that bear most directly on a law firm's use of an outside service provider:

- **Formal Opinion 477R** (2017), Securing Communication of Protected Client Information
- **Formal Opinion 483** (2018), Lawyers' Obligations After an Electronic Data Breach or Cyberattack
- **Formal Opinion 498** (2021), Virtual Practice
- **Formal Opinion 512** (2024), Generative Artificial Intelligence Tools

Each section answers the questions those opinions direct you to ask, in the order a careful reviewer tends to ask them, and states operating facts specific enough to be checked rather than comfortable claims that cannot be.

> ### On credentials we do not hold
>
> Sum Certain holds no third-party security credential such as SOC 2, and claims none. A practice of this size cannot honestly hold one. What follows instead is a plain description of how the practice actually operates, stated specifically enough that your firm can hold us to it.

THE PRACTICE AT A GLANCE

The facts, in one place

Legal entity	Sum Certain LLC, a Washington limited liability company
Principal	Josh Hsu, founder
Service	Monthly bookkeeping and three-way IOLTA trust reconciliation for US law firms of 2–10 attorneys
Delivery	Fully remote, United States
Systems of record	QuickBooks Online, alongside Clio or LeanLaw where the firm already uses them
Published method	The Three-Way Standard, at getsumcertain.com/methodology
Published pricing	Flat monthly tiers, at getsumcertain.com/pricing
Contract	Month-to-month, 30 days' notice
Insurance	Professional liability $1,000,000 each claim / $1,000,000 aggregate; cyber $250,000 each claim / $250,000 aggregate. Carrier Hiscox, effective August 1, 2026. Certificates of insurance available on request.
Out of scope	Tax return preparation, and any engagement requiring a license the practice does not hold

SECTION 1

Client funds: what we can and cannot do

The most important control in this packet, and the one that determines your firm's risk exposure more than any other: Sum Certain never has custody of client funds.

- We work from official monthly bank statements and **read-only** bank access.
- We **cannot** move money, initiate transfers, disburse, or approve a disbursement from any account, trust or operating.
- We are not a signatory on any client account, and will not accept signatory authority if it is offered.
- Your firm remains the only party that can move client money. We record and report on it.

> ### Why this belongs in your file
> A bookkeeping provider holding payment authority is a materially different risk than one that cannot move a dollar. Sum Certain is structurally in the second category by design, and will not move into the first. If a future provider asks your firm for disbursement rights, that difference is the question to ask.

The control your trust account gains

Trust rules assume a second set of eyes on the money. Where one person at a firm both moves funds and records them, an error has nowhere to be caught. Engaging an outside reviewer separates those roles: the party that moves client money (your firm) is never the party that reconciles it (us). That independence exists from the first month of an engagement, and it is the reason the arrangement improves your position rather than simply relocating the work.

SECTION 2

Confidentiality and communications

Maps to ABA Formal Opinion 477R (2017)

477R asks whether the security applied to client information is proportional to its sensitivity, communication by communication, rather than assuming any single method is always sufficient. Trust records sit at the sensitive end of that range.

How information moves

- **Encrypted document exchange.** Statements and supporting documents move through an encrypted client portal, never as email attachments.
- **Email is for coordination, not records.** Client-identifying trust records are not sent or requested by email.
- **Intake discipline.** The practice's own contact form asks for no trust-account details, client names, or matter information. We do not collect what the work does not require.

How access is controlled

- **Multi-factor authentication on every tool** in the practice's stack. No shared logins, no exceptions.
- **Least-privilege scope.** Access is limited to what the work requires: read-only bank access, your accounting file, and the documents you share.
- **Reviewed at both ends.** Access is reviewed when an engagement begins and removed when it ends, with removal confirmed in writing.
- **US-hosted systems.** Core systems for accounting, document exchange, and email are hosted with US-based providers under US data terms.
- **Confidentiality in writing.** Every engagement letter carries a confidentiality commitment covering your firm's and your clients' information.

Devices

Work is performed on practice-controlled devices with full-disk encryption, automatic screen lock, and MFA on every account reachable from them. Client records are not kept on personal or shared devices.

SECTION 3

Remote practice and supervision

Maps to ABA Formal Opinion 498 (2021)

498 addresses virtual practice: where the work happens, who actually performs it, and how it is supervised. These are fair questions to ask a remote provider, and vague answers are the reason they get asked.

Who performs the work

Today: Josh Hsu, personally. The practice has no employees and no contractors. If that changes, the person will be **named on the public security page** at getsumcertain.com/security, bound by the same written confidentiality terms, and disclosed to active clients. There will be no anonymous team downstream.

Supervision and sign-off

Every three-way reconciliation is reviewed and signed by Josh Hsu before it reaches the client. The sign-off is timestamped and logged. This is the practice's core control, and it does not change with capacity: a person, not a pool, signs the reconciliation.

> ### Segregation of duties, stated precisely
>
> **Between your firm and the practice (in place today):** the party that moves client money is never the party that reconciles it. This is the segregation that protects your trust account, and it exists from month one.
>
> **Within the practice (future state):** when capacity is added, preparation and review will be split between two people. Today the founder performs the work and reviews it. The compensating controls are the published method, the timestamped sign-off log, the monthly evidence archive, and the exception register, all described in The Three-Way Standard.

Continuity

The practice is deliberately small, and what happens if the principal is unavailable is a fair question to ask. Your firm's protections here are structural rather than promissory: month-to-month terms with 30 days' notice, books and working papers handed over in a standard portable format on request, and the fact that you always hold your own copy. A named backup reviewer, bound by the same written confidentiality terms, is arranged as the practice grows.

SECTION 4

Artificial intelligence policy

Maps to ABA Formal Opinion 512 (2024)

512 asks lawyers to understand and supervise the generative AI in their supply chain, including their vendors'. Silence on this question reads as concealment, so here is the whole policy in five lines.

— **No AI system prepares, computes, reviews, or approves your reconciliation.** A person does, and signs it. That does not change as tooling changes.

— **Client records never enter public or consumer AI tools,** and are never used to train any model. This includes statements, ledgers, client names, and matter information.

— **Where AI-assisted tooling is used beyond features built into licensed software,** it runs on private, US-hosted commercial systems under a signed data processing agreement with zero data retention. Anthropic is the only such provider and is named in the subprocessor table.

— **Every entry is verified against its source document** before it is recorded, whether or not any tool suggested it, and the reconciliation is reviewed and signed by a person regardless.

— **If this policy changes, it changes publicly first,** on the security page, and active clients are told.

SECTION 5

Incident response and notification

Maps to ABA Formal Opinion 483 (2018)

483 governs what happens after an incident, and it makes your firm's own notification obligations depend partly on how quickly your vendor tells you.

- **Notification without delay.** If the practice becomes aware of a security incident involving your firm's or your clients' information, we notify your firm's designated contact in writing promptly, and in any event within **72 hours** of confirming the incident.
- **We do not wait for a complete investigation.** We notify on confirmation and update as facts develop; a tidy final report is worth less to you than early warning.
- **What the notice contains:** what happened, when, what information was involved, what has been done to contain it, and what we recommend your firm do.
- **Preservation.** Relevant logs and records are preserved so your firm can meet its own obligations to clients and to the bar.
- **Your books remain available.** An incident at the practice does not leave your firm without its records. See Records and exit.

SECTION 6

Subprocessors

The practice's operating stack as of this version. Any addition that would touch client information is disclosed to active clients before it is used.

PROVIDER	PURPOSE	CLIENT TRUST DATA
Intuit QuickBooks Online	Accounting system of record	Yes: the firm's books
LeanLaw	Trust and IOLTA workflows inside the firm's QuickBooks file	Yes: trust and matter data
Clio or CosmoLex	Read-only access to practice-management data, only where the firm already uses them	Yes: under the firm's own account
Financial Cents	Practice workflow, client tasks, and the reconciliation sign-off log	Client names and task status
Dext and Uncat	Receipt capture and uncategorized-transaction queries	Yes: transaction data
Anchor	Proposals, e-signature, billing, and encrypted client document exchange	Yes: statements and supporting documents shared by the firm
Anthropic	AI-assisted drafting and flagging items for review, under a signed data processing agreement with zero data retention. Never computes or approves a reconciliation.	Limited, under commercial terms; never used for training
Google Workspace	Practice email and internal document storage	Yes: documents and correspondence
Mercury	The practice's own business banking, which receives your payment for our services	None: no client books, matters, or trust data
Netlify, Formspree, Calendly	Website hosting, contact-form delivery, call scheduling	None: the forms request no client information

SECTION 7

Records, retention, and exit

Your records are yours. This is written into the engagement letter and repeated here so it is in your file.

- **You always hold your own copy.** The practice is never the sole custodian of your firm's records.
- **On termination, for any reason,** the practice hands over complete and current books and working papers in a standard, portable format.
- **Access is removed at the same time,** on the practice's side, and removal is confirmed to you in writing.
- **Retention.** Records are retained per the engagement letter. Where your state imposes a longer period on your firm's trust records (Washington's RPC 1.15B, for example, requires seven years), the monthly evidence archive is built to support that obligation, not to replace your own copy of it.
- **Notice.** Month-to-month, 30 days. No termination penalty, no minimum term.

CLOSING

Holding us to it

A diligence packet is only worth the ease of checking it. Everything here is stated publicly, so nothing in this document depends on your taking our word for it in private.

Verifying any of this

Every claim in this packet is also stated publicly at getsumcertain.com/security and getsumcertain.com/methodology. If a statement here and a statement there ever disagree, that is a defect in our records, and we would like to know about it.

Questions this packet does not answer: **hello@getsumcertain.com**. No form required, and a reply the same business day.

This packet describes the operating practices of Sum Certain LLC as of the version date. It is provided for your firm's vendor-diligence file and is not legal advice. It does not by itself discharge your firm's obligation to evaluate a service provider; it supplies facts, and the judgment remains yours. Sum Certain provides bookkeeping and advisory services and is not a licensed CPA firm. Reviewed quarterly; the current version is always available at getsumcertain.com/security.