Active File Review

Premium intake-to-completion workflow for one-off responses to IRCC, CBSA, IRB, and ESDC notices. AI-extracted metadata from the client's uploads, three platform pathways plus a custom escape valve, one-click Service Agreement generation, automatic Bill on signing, encrypted client portal with OTP, and a thirty-day audit-trail close.

Up to date as of v1.32.0

CONTENTS

- Overview
- Important: read before using
- Share the intake URL
- Share in another language
- Embed the intake on your website
- Language Settings
- Bill on signing
- The AFR list page
- The public intake form
- The three pathways plus Custom
- Triage the matter
- Accept and the seven-item checklist
- Decline and the structured reason
- Request more information
- Override pathway or price
- Convert to custom Service Agreement
- Generate the Service Agreement
- Automatic Bill on signing
- Payment received and the receipt
- The client portal
- Deliverables and Mark complete
- The thirty-day close
- Encryption and storage
- Audit and the events ledger
- Notifications when the client acts
- Integrations with other modules

Overview

Active File Review (AFR) is the module you reach for when a prospective client arrives with an open immigration matter that needs a specific, time-bounded response. The canonical examples are a Procedural Fairness Letter from IRCC, a refusal letter, an inadmissibility allegation, an invitation to an interview, or an additional-document request. The client lands on your public intake form, uploads the authority's letter plus any supporting documents, types a short narrative, and submits. The platform's AI extracts metadata (authority, issue type, application number, response deadline) from the uploaded letter, encrypts every byte under your tenant key, and lands the matter on your dashboard as a triage card. From there you Accept, Decline, ask for more information, or override the suggested pathway and price.

The accounting model has three distinct artifacts. A Payment Request is what you send post-signing but pre-work: it collects funds into your trust account but is not the final invoice. A Receipt is issued when payment is received and marks the moment your client portal opens. An Invoice is issued when the work is completed (or a milestone is reached) and records the fact that fees have been earned and may be transferred from trust to general. The platform records every transition with timestamps so an audit trail exists even when nothing has yet been emailed.

> **Premium**: Active File Review is Premium. Basic tenants see the sidebar entry and the dashboard tile; clicking lands them on a Premium upsell card with a direct subscribe link. Once subscribed, every feature in this chapter unlocks, including AI document extraction, the encrypted client portal, the multilingual public intake, the auto-bill bridge, and the thirty-day close-of-case flow.

What ships in this module

- A public, anonymous intake form addressed by your firm's slug, available in EN and fr-CA plus eight run-time-translated languages on Premium.
- Signed-URL direct uploads from the client's browser to encrypted storage, bypassing the 4.5 MB serverless body cap so large IRCC letter packages succeed.

- AI extraction (Gemini 2.5 Flash) of authority, issue type, application number, response deadline, and triage summary from the uploaded authority letter.
- Three platform pathways (Review and Advice, Prepare a Response, Full Representation) plus a Custom pathway escape valve for matters that don't fit.
- One-click generation of a pre-filled Service Agreement from the AFR card, with the AFR fields auto-mapped into the SA draft and a source pointer linking the two rows.
- Automatic Bill creation when the SA reaches fully-signed (when global Bill on signing is on), routing funds collection through Stripe or any offline method you have configured.
- OTP-gated client portal that opens on payment receipt, where the client uploads additional documents and downloads the deliverable when you mark the case complete.
- Thirty-day audit-trail close: the cron automatically flips the case to closed at day 30 but keeps the portal accessible for archival download.

Important: read before using

> **Important**: Active File Review is a workflow tool. It is not legal advice, not a substitute for licensee judgement, and does not represent the client to any authority on its own. Every pathway eventually generates a Service Agreement that you, the RCIC of record, sign and execute. The AI extraction is a triage helper, not a citation-bearing legal opinion: you review and confirm every field on the dashboard card before accepting.

The accounting language matters. A Payment Request is not a payment demand on an invoice; it is the document that funds collection BEFORE work begins. A Receipt is what your client receives when their payment lands. An Invoice is the record that work has been done and fees are earned (often referred to as the trust-to-general transfer authorization). When you reach the close-of-case flow, the Invoice is a RECORD DOCUMENT, not a

charge — the money was already collected at the Payment Request stage and sat in trust through the work. Do not add a Pay-invoice button or any second-payment surface on the Invoice. Doing so would re-bill a client who already paid.

AFR records operational milestones (payment received, receipt issued, invoice issued, fee earned, trust-to-general transfer marked). It does not implement bank reconciliation, general-ledger posting, or split disbursement. The trust-to-general transfer is a tenant-facing marker only; the platform records the marker, but you actually move bank funds out of band, per your firm's procedures and your jurisdiction's trust accounting rules.

Share the intake URL

The first card on the AFR dashboard is the intake-URL share card. It carries your firm's public intake URL in the form https://rcicapp.ca/active-file-review/intake/<your-slug>, a Copy URL button, a Share in another language disclosure, and a Show iframe embed code disclosure. The URL is the only thing your client needs to land on the intake form; share it via email, on your website, in a social-media post, or printed on a business card.

The URL is public but unguessable for tenants whose slug is non-obvious. Anyone who has the URL can submit an intake; there is no per-client token at the intake stage (the per-client portal opens only after acceptance and payment). The URL is robots-blocked at our end so search engines do not index it, but your client can paste it into any browser, email client, or messaging app and it will resolve.

Share in another language

Click Share in another language on the intake-URL card to expand a dropdown of the languages your tenant has enabled. Pick a language and the platform appends ?lang=<code> to the intake URL so the page renders directly in that language when your client opens the link (no manual picker click needed). English and Quebec French are always available because the intake copy is hand-curated in both. Premium tenants additionally see Spanish,

Simplified Chinese, Punjabi, Arabic, Hindi, Tagalog, Urdu, and Farsi, all rendered at request time through Google Translate against the same EN canonical source.

The eight runtime-translated languages are derived from the language set on your booking page (Settings -> Premium -> Languages). If you want a language available on the AFR intake but you do not have it ticked there, tick it on the Premium settings page first. The set is shared across modules so a tenant who serves a Punjabi-speaking client base ticks Punjabi once and the AFR intake, the booking page, the Personal Invites surfaces, and other client-facing language pickers all honour it.

> **Note**: The client can still override your shared language by clicking the picker on the intake page itself. The ?lang= URL parameter sets the initial value; the picker lets the visitor pick a different one. This matters when a parent and child share the link and prefer different languages, or when a client opens the link in a browser whose system language is different from what you shared.

Embed the intake on your website

Click Show iframe embed code on the intake-URL card to reveal a copy-ready HTML snippet. The snippet wraps the intake page in an iframe sized to one hundred percent width and a generous minimum height (currently 1400 pixels) with lazy loading and an accessible title. Paste it on any page of your website and your visitors fill the intake form without leaving your site. The page detects the embed mode via a ?embed=1 query parameter and drops the full-screen grey background, the marketing header, and the Powered-by footer so the form renders edge-to-edge in your layout.

When you embed, the same language behaviour applies. Append ?lang=fr or another supported code to the iframe src so that the embedded form opens in that language directly. If your website itself is multilingual, link to two different copies of the snippet (one per language) from the two language versions of your page.

> **Note**: The 1400-pixel minimum height accommodates the full nine-step wizard plus the post-submit confirmation panel without an inner scrollbar on typical desktop layouts. If your site layout forces a smaller container, you can raise the min-height or remove it entirely; the iframe will simply expand as the visitor moves through the steps (cross-origin iframes do not auto-resize, so you cannot shrink it dynamically without a postMessage bridge that we do not ship in v1).

Language Settings

The Language Settings link in the AFR sidebar is a deep link to your Premium settings page where you tick which of the ten supported languages your tenant publishes to clients. The link exists because tenants typically discover the language picker only when they need to share their intake URL with a non-English-speaking client. The list there governs three surfaces at once: the AFR intake page, the AFR client portal, and your public booking page. Tick a language once and every client-facing surface honours it.

English and Quebec French are always available because the intake and portal copy are hand-curated in both. The other eight (Spanish, Simplified Chinese, Punjabi, Arabic, Hindi, Tagalog, Urdu, Farsi) render at request time through Google Translate against the same EN canonical source. The translation is good for everyday immigration vocabulary but not a substitute for a sworn translation when one is required; the intake page surfaces a small disclaimer to that effect when a non-EN, non-FR locale is active.

> **Premium**: The eight runtime-translated languages are Premium-only. Basic tenants stay on EN + fr-CA across every client-facing surface. If a Basic tenant deep-links into the language settings page, they see the Premium-discovery card with a direct subscribe link.

Bill on signing

Bill on signing is a global setting that lives on your firm's billing profile, not on individual AFR matters. When it is on (the default), the platform auto-creates a Bill the moment any Service Agreement reaches fully-signed status — including the SA your AFR generated. The Bill is emailed to the client with a Stripe Checkout link and (if you have configured them) wire/cheque/e-Transfer/cash payment options. The setting also drives a daily reminder cron that nudges unpaid Bills along on a tenant-configurable cadence.

The AFR list page surfaces the current state of Bill on signing in a banded card right below the intake-URL share card. When the setting is on, the card is emerald with an Active pill and an explanation that automatic billing applies to every fully-signed SA, including AFR matters. When the setting is off, the card is amber with an Off pill warning that AFR matters will not auto-bill; you will need to issue bills manually from Single Bills after each SA signs. Click Configure billing on signing to land on the SA module's billing-settings page where the toggle lives.

> **Important**: Bill on signing is a global setting that applies to every Service Agreement your firm signs, including AFR-sourced ones. Turning it off because one AFR matter needs special handling will also stop auto-billing on every other SA you sign that day. If you want to suppress auto-bill for one specific matter, cancel the auto-generated Bill from Single Bills after the SA signs (it is created at fully-signed, not at draft) and issue a manual bill with the special terms instead.

The AFR list page

The list page at /dashboard/active-file-review shows every matter that has reached your firm via the intake form, ordered most recent first. Above the table you find the intake-URL share card, the Bill on signing status card, and a filter bar with five chips: Status, Authority, Pathway, Urgency, and Assigned RCIC. Each row carries the client name (decrypted server-side from the encrypted column), the authority (IRCC, CBSA, IRB, ESDC, or Other), the issue type, the response deadline with an urgency badge (Urgent, Tight, Normal, or Unknown), the pathway pick, the status pill, and the date the intake was submitted. Click any row to land on the matter detail page.

Status pills, in order

- Submitted: the intake just arrived; you have not reviewed it yet. Charcoal.
- Needs more info: you sent the client a continuation link asking for clarification. Amber.
- RCIC reviewing: a triage marker you can set manually while you work through the file. Blue.
- Declined: you have formally declined; the client received a structured decline email. Charcoal.
- Accepted - generate SA: you have accepted; the next action is to click Generate Service Agreement. Emerald.
- Price negotiation: you proposed a price change and the client is deciding. Amber.
- SA generated / SA sent / SA signed: the Service Agreement is in the canonical SA module lifecycle. Maroon.
- Payment request issued: the auto-bill has fired (or you have issued a manual bill); funds are pending. Blue.
- Portal open: payment received; the client's portal is now accessible with OTP. Emerald.
- In progress / Waiting for client / Deliverable ready / Client acknowledged: the work-phase substates. Blue.
- Invoice issued / Fee earned / Completed: you have marked the case complete; the trust-to-general transfer marker is set. Emerald.
- Closed: the thirty-day archival window expired; the portal stays accessible but the case is archived. Charcoal.
- Cancelled: you cancelled the matter at any prior stage. Charcoal.

The public intake form

When your client lands on the intake URL, they see your firm's name and logo, a brief explanation of what an Active File Review is, and a multi-step form. They identify themselves (name, email, phone), pick the authority that issued the letter, type a short narrative of what the letter says and why they need help, declare the response

deadline if they know it, and upload the letter plus any supporting documents. The form is bilingual EN + fr-CA out of the box; Premium tenants get eight more runtime-translated languages via the picker.

The form's submit button is disabled until every required step is complete: identification, authority, narrative, at least one uploaded file (the authority letter is required), and the client's typed acceptance of the platform's privacy notice. Submit triggers a server-side encryption pass: client name and email land on the encrypted columns + blind-index hash columns; uploaded bytes land on the encrypted storage bucket under your tenant data-encryption key (DEK); the typed narrative is encrypted as JSON. The success page tells the client what to expect next (you will review their file and reach out within your firm's typical turnaround window) and offers a continuation link they can save in case they need to add more documents later.

Signed-URL direct upload

Files do not transit our serverless function on the way in. Each upload mints a signed URL on demand, and the browser PUTs bytes directly to Supabase Storage. This bypasses the 4.5 MB body cap Vercel enforces on serverless function requests and means large IRCC packages (full disclosure bundles, certified copies of identity documents, refusal letters with extensive appendices) succeed cleanly. Per-file cap is 50 MB; total intake cap is 150 MB. Server-side validates both caps before issuing the signed URL.

AI document extraction

After upload, the platform runs the uploaded authority letter through Gemini 2.5 Flash with a structured-output prompt that extracts authority (IRCC, CBSA, IRB, ESDC, or Other), issue type (Procedural Fairness Letter, refusal, inadmissibility allegation, invitation to interview, additional document request, or Other), application or file number, response deadline (with a deadline-confidence score), and a one-paragraph triage summary. The extraction is a hint, not a citation-bearing legal opinion. You see the extracted values on the dashboard card and confirm or correct each one before accepting. The triage summary is the AI's read of what the letter says; you read the actual letter before acting on it.

The three pathways plus Custom

Every AFR carries a pathway pick that frames the scope and price for the Service Agreement we will generate. There are three platform pathways plus a Custom escape valve. The client picks an initial pathway on the intake form based on a plain-language description; you can override the pick on the dashboard before generating the SA.

Pathway 1 — Review and Advice

The lightest pathway. You read the client's file and the authority's letter, and write back an advice memo: what the letter is asking, what the client's options are, what risks each option carries, and what your professional recommendation is. The client implements (or does not implement) the advice themselves. Platform-default price is $99 CAD. The generated Service Agreement template carries a scope clause naming the advice memo as the sole deliverable; you do not file anything with the authority on the client's behalf under this pathway.

Pathway 2 — Prepare a Response

You prepare the response (the PFL rebuttal, the refusal-letter reply, the requested supporting evidence) and hand the prepared package to the client. The client files it themselves with the authority, in their own name, under their own signature. The platform-default price is $499 CAD. The generated SA template carries a scope clause that names the prepared response package as the deliverable and explicitly states that the client remains the filer of record.

Pathway 3 — Full Representation

You take over the matter. You sign and file the IRCC Use of Representative (IMM 5476) form, you become the representative of record for this stage of the matter, you communicate with the authority directly, and you carry the matter through to the final outcome at this stage. The platform-default price is $999 CAD. The generated SA template carries a full-representation scope. The slug for this pathway is historically named limited_representation in the database (the original product name before the scope was widened); the user-facing label everywhere is

Full Representation. Do not be confused if you see the legacy slug in audit logs or operator surfaces; the meaning is full takeover.

Custom pathway

When none of the three platform pathways describes the matter (for example a hybrid scope, a multi-stage engagement, or a matter that needs unusual terms), use the Custom pathway. The Custom pathway skips the template auto-apply step; you draft the Service Agreement from scratch in the SA Builder. You can either pick Custom on the intake form before submitting, or use the Convert to custom Service Agreement action on the dashboard to switch a previously-picked platform pathway into Custom (useful when the AI extraction missed a wrinkle and you only spot it during triage).

> **Note**: Platform prices are starting points, not floors or ceilings. The Override price action on the dashboard lets you set any non-negative amount for any matter; the override flows through to the auto-generated Service Agreement. A price change AFTER the client has already seen the original price requires the client's consent through the price-negotiation flow.

Triage the matter

Click an AFR row from the list to open the matter detail page. The page is dense by design: header with client name, authority, and issue type plus the current status pill; an action bar with the four primary actions (Accept, Decline, Request more information, Change pathway / Override price / Convert to custom); a left column carrying the client identity card, the matter card, the pricing card, the AI summary card, the client's typed narrative card, and the continuation transcript card; a right column carrying the documents card (every upload with a per-row Download button) and the audit ledger card (every event with timestamp, actor, and IP redacted to /24). Everything in the left column is decrypted server-side per request.

Triage is your moment to confirm what the AI extracted. Read the actual authority letter (use the Download button on the documents card). Compare the AI's extracted authority, issue type, application number, and response deadline against what the letter says. If something is wrong, the matter card and pricing card both let you edit in place. Read the client's typed narrative. Read the AI summary as a second opinion, not as a substitute for your own reading. When everything looks right and you are ready to take the matter, click Accept and continue.

Accept and the seven-item checklist

The Accept modal carries a seven-item professional-responsibility checklist that you tick before the action will fire. Each item maps to a Code of Professional Conduct due-diligence question you should have already answered in your head before getting this far; the checklist makes that diligence explicit and records it on the audit ledger. The seven items: you have read the authority's letter in full, you have the capacity (time, skill, resources) to handle the matter within the deadline, the scope and pathway you have chosen are appropriate, the price is appropriate, there are no conflicts of interest, the client is eligible for the service you intend to render, and you have noted any limitations or assumptions you are relying on.

Confirming Accept advances the status to Accepted - generate SA and writes an acceptance_checklist event to the audit ledger with each ticked item recorded. The platform now expects the next action to be Generate Service Agreement. The acceptance checklist card stays visible on the detail page as a permanent record of which items you ticked and when.

Decline and the structured reason

The Decline modal carries a required dropdown of structured reasons: deadline too short, outside scope, requires a lawyer referral, conflict or existing-representative issue, missing documents, client not eligible for this service, requires a custom quote, not a service the tenant offers, capacity unavailable, or Other. Picking Other reveals a required notes field. The chosen reason and any typed notes are encrypted under the tenant DEK and recorded

on the audit ledger. The client receives a bilingual decline email that names the reason in plain language and offers any next steps you noted.

Declining is a terminal action by design. There is no Reopen button. If you decline and then change your mind, you can have the client submit a fresh intake (no platform restriction prevents this). Code section 7 obligations around providing reasons for declining a retainer are satisfied by the structured email plus the audit-ledger record of which reason you picked.

Request more information

When the intake is incomplete, click Request more information. The modal asks what specific information you need (free text, encrypted on save). On submit, the platform mints a one-shot continuation token (32-byte CSPRNG hashed before persisting; plaintext never lives in the database), emails the client a continuation link valid for fourteen days, and flips the status to Needs more info. The client clicks the link, lands on a lightweight surface at /active-file-review/continue/<token> where they can upload additional documents and answer your free-text question, and submits. The token burns on submit (no re-use possible), the additional uploads encrypt into the same bucket folder as the original intake, the answer joins the continuation transcript, and the status reverts to Submitted with an audit-ledger entry of the round trip.

The continuation surface is intentionally lightweight: additional uploads and a typed answer, nothing else. No deliverables, no portal session, no payment surface. It exists solely to close the gap between an incomplete intake and your decision to Accept or Decline. You can issue multiple continuation requests on the same matter (each mints a fresh token; the previous one is invalidated). The continuation transcript card on the dashboard shows every round trip in chronological order.

Override pathway or price

Two override actions live on the matter detail page and apply before the Service Agreement is generated. Change pathway lets you switch between Review and Advice, Prepare a Response, Full Representation, and Custom; the new pathway's default price loads automatically unless you have already overridden the price. Override price lets you set any non-negative dollar amount for the matter; the override flows through to the generated SA's professional fee.

Price changes after the client saw the original

If the price has changed since the client submitted (in either direction — increase or decrease), the system routes the change through a consent flow rather than writing it silently. The status flips to Price negotiation and the platform mints a one-shot decision token, then emails the client a bilingual proposal with three options: Accept (the new price applies; the matter reverts to its prior status and continues toward SA generation), Decline (the new price is rejected; the original price stays; the matter reverts to its prior status with no other change), or Discuss (the client asks to talk before deciding; the matter stays in Price negotiation and you handle the conversation out of band). You can also Cancel the pending proposal from the dashboard at any time, which reverts the matter to its prior status without applying the new price.

> **Note**: Both directions need consent — an unexpected decrease is also a price change the client should know about (it might mean the scope is smaller than they expected, which is informationally material even when financially favourable). The flow exists because re-pricing silently after a client has already seen one number is a CICC consumer-protection risk; making the consent explicit eliminates it.

Convert to custom Service Agreement

Sometimes the AI extraction picked a pathway that fits at first glance but does not survive triage. Convert to custom Service Agreement is the escape valve: it switches the pathway to Custom in one click, which means the next Generate Service Agreement action will skip the template auto-apply step and drop you into the SA

Builder with a blank canvas (other than the client and matter fields the AFR auto-fills). Use this when the matter has hybrid scope (advice + drafting), multi-stage handoff (response now, follow-on filing later), or unusual terms (a retainer-style arrangement, a contingent fee that needs unusual disclosure, or an out-of-jurisdiction subject matter where you need extra language).

The Convert action is one-way. Once converted to Custom, you cannot switch back to one of the three platform pathways from this matter. If you have already started filling out the Custom SA and decide the platform pathway was actually right after all, your best move is to discard the Custom draft (Delete agreement on the SA detail page) and re-start by changing the pathway back to its platform pick before clicking Generate Service Agreement again.

Generate the Service Agreement

Once the matter is in the Accepted - generate SA status, click Generate Service Agreement. The platform decrypts the AFR's client identity (name, email, phone, address, date of birth, citizenship), the matter framing (authority, issue type, application number, response deadline), and the chosen pathway and price, then writes a fresh Service Agreement row with everything pre-filled and a source pointer (source_kind set to active_file_review, source_id set to the AFR row id) linking the two records. For the three platform pathways, the matching SA template is auto-applied, which fills the scope and clause body from the curated platform copy. For Custom, the template step is skipped and you write the scope yourself in the SA Builder.

When your firm has more than one verified RCIC and the platform cannot infer which one should be the main RCIC of record, the Generate modal first presents a Pick the RCIC picker that lists every eligible member. Pick one and the SA is generated under that RCIC's name. From the moment the SA exists, the canonical work surface for this matter is the SA detail page at /dashboard/agreements/<id>. The AFR detail page surfaces an Open the Service Agreement draft link in the action bar so the round trip is one click.

The SA detail page is the canonical Service Agreement workspace: validator, builder, parties, signing portal token mint, signed-PDF storage, audit ledger, and the rest of the SA module's surface. Everything you do there (sending for signature, the client signing, the RCIC counter-signing, the eventual signed-fully event) writes back to the AFR row via the source pointer. AFR status transitions from sa_generated to sa_sent to sa_signed track the SA's lifecycle so the AFR dashboard stays a useful at-a-glance view even after the work moves to the SA module.

Automatic Bill on signing

When the Service Agreement reaches fully-signed and your global Bill on signing setting is on, the platform automatically creates a Bill in the Single Bills module and emails it to the client. The Bill's amount equals the SA's professional fee (the AFR's price, or your override of it). The Bill body and email subject identify the matter by AFR reference and link back to both the SA and the AFR. Payment options are whatever you have configured in your firm's billing profile: Stripe Checkout always (when your Stripe Connect account is active), plus any of e-Transfer, cheque, wire transfer, and cash you have ticked.

The Bill's record is the Payment Request artifact in the AFR accounting model. The matter status flips from sa_signed to payment_request_issued. The payment card on the AFR detail page shows the Bill amount, the issue date, the payment status (Unpaid / Paid by Stripe / Paid offline), and a link to the Bill record itself in the Single Bills module. You can issue a manual Bill out of cycle if needed (the Bill on signing setting was off when the SA signed, or you want to issue a partial Bill before the SA signs); use the Single Bills module's Create bill action and reference the AFR matter in the description.

> **Note**: If your firm has configured an Accountant CC address (Settings -> Billing -> Notify the accountant), every Bill — including the AFR auto-bill — is CC'd to your accountant's address. This means your bookkeeper sees the Bill at the same moment the client does, which closes the time gap between work-billed and work-recorded in your firm's books.

Payment received and the receipt

When the client pays through Stripe Checkout, Stripe's webhook fires our handler and the system performs a single atomic UPDATE that advances the AFR from payment_request_issued to portal_open, stamps payment_received_at and receipt_issued_at and portal_opened_at, mints a fresh portal token, and sends the client a bilingual receipt email with the new portal link. The receipt names the matter, the amount paid, the date of payment, and the firm's CICC name and number. Offline payments (e-Transfer, cheque, wire, cash) follow the same logic when you Mark as paid on the Bill in Single Bills — the system does not distinguish payment channel for the AFR-side state transition.

The token rotation matters: the receipt email's portal link is what the client uses from now on. Any prior link the client might have (from a payment-confirmation email or a prior continuation request) no longer resolves. This is intentional — the moment of payment is the right moment to give the client a fresh capability that they can save and re-use throughout the work phase. The status pill on the AFR detail page flips to a green Portal open badge so you can see at a glance which matters are ready for active work.

The client portal

The client portal at /portal/afr/<token> is the OTP-gated workspace where your client uploads additional documents during the work phase and downloads the deliverable once you mark the case complete. On first visit (or after the 30-minute idle window expires), the page presents a two-stage OTP gate: the client confirms their email matches the email on file, the platform sends a six-digit code to that email, the client enters the code. On success, an HMAC-signed session cookie is issued for that browser, valid for thirty idle minutes and refreshing on every interaction.

The session cookie is scoped to the AFR portal specifically (a versioned domain prefix in the HMAC payload) so a token signed for a Transfer Room portal session cannot be replayed against an AFR session and vice versa.

Lockout and cooldown rules apply on the OTP gate: five wrong codes lock the email for ten minutes, sixty-second cooldown between successful sends, ten OTPs per email per day. These limits are per-email not per-IP, so an attacker who guesses one client's email can probe the OTP gate but cannot brute-force the six-digit space at scale.

What the client can do in the portal

- See the matter summary: client name, authority, issue type, response deadline, status, the firm's CICC name and number.
- Upload additional documents through the same signed-URL pattern as the intake (per-file 50 MB cap, encrypted under the tenant DEK at upload time).
- Download deliverables you have uploaded once you mark the case complete.
- See a redacted timeline of platform events on the matter (every status change, every deliverable upload, every Mark complete event).
- Request to change the email on file via the verify-before-swap flow (the new address must confirm via OTP before the old address loses access; both addresses receive a notification of the change).
- Sign out (the cookie is cleared; the URL token still resolves so the client can re-OTP later from the same link).

Deliverables and Mark complete

When your work on the matter is done, click Mark case complete on the matter detail page. The modal lets you upload deliverable files (the advice memo for Pathway 1, the prepared response package for Pathway 2, the filed-with-the-authority confirmation for Pathway 3, whatever your custom matter produced for Custom), type an optional summary your client will see in the portal, and pick a deliverable type from the structured enum (advice memo, document checklist, response letter, final response package, reviewed document list,

representation takeover instructions, withdrawal recommendation, next-steps memo, other). Each uploaded deliverable is encrypted under the tenant DEK and stored in a deliverables sub-folder of the AFR's storage path.

On submit, the platform writes the Invoice artifact: a stamped invoice_issued_at, an invoice_id (a UUID, not a Stripe artifact — the Invoice is a record document, not a charge), and a fee_earned_at flag indicating that the fees are now considered earned and the trust-to-general transfer is authorized. The matter status flips to Completed. The portal token rotates again so the case-completed email's link is the canonical one going forward. The case-completed email carries the deliverable files as attachments (or as portal links if any individual file exceeds the platform's email-attachment threshold) and tells the client the case is now complete with a thirty-day window to download anything they want to keep.

> **Important**: The Invoice generated here is a record document. The money was already collected at the Payment Request stage and has been sitting in your trust account through the work phase. The Invoice records that the work is now done and the funds may be transferred from trust to general per your firm's procedures and your jurisdiction's trust accounting rules. Do not interpret the Invoice as a second payment demand; do not send the client a follow-up asking them to pay it.

The thirty-day close

Twenty-five days after Mark complete, a cron fires a final-reminder email to the client noting that the matter will close in five days and reminding them to download anything they want to keep. The portal token rotates again at this point so the reminder email's link is fresh. Thirty days after Mark complete, a second cron flips the matter status to Closed. The portal stays accessible — the URL still resolves, OTP still works, the client can still download every deliverable indefinitely — but the matter is now archived from your active-list perspective and no further status changes are possible without operator intervention.

The deliberate design: Closed is an archival state, not a revocation state. Your client retains audit-trail access to the deliverables you produced for them, forever. This satisfies the Code's record-keeping and client-access obligations without requiring a separate vault product or a long-tail download surface. The matter no longer surfaces on your default AFR list (you filter to status = Closed to see it), but the data lives on and the client retains read access via their original portal URL.

Encryption and storage

Every byte of client PII and document content in the AFR module is encrypted at rest under your tenant data-encryption key (DEK), which is itself wrapped under a master key-encryption key (KEK) that lives in Vercel environment variables (not in the database). Client name and email land on encrypted columns plus blind-index hash columns (HMAC-SHA256 under a separate search-index key, base64 encoded) so we can do exact-match lookups without ever decrypting the canonical value. Document bytes land on a dedicated private storage bucket with no public read policy; the per-byte content type is forced to octet-stream so a leaked URL does not let a browser auto-render an attached PDF or image preview.

Decryption happens server-side on a per-request basis when an authorized actor (you, your assistant on this matter, or the client through their OTP-gated portal session) needs to see a value. The decrypted stream is discarded immediately after the response completes. Even an attacker with full database and storage access cannot read client names, emails, narratives, or document content without also obtaining the master KEK from Vercel — and the KEK rotation procedure does not require us to re-encrypt your data (only to re-wrap the per-tenant DEK), so a compromised KEK has a fast recovery path.

Audit and the events ledger

Every state change on an AFR matter writes a row to the events ledger: intake_submitted, ai_extracted, additional_info_received, accepted, declined, price_change_proposed, price_change_accepted, price_change_de-

clined, price_change_negotiation_requested, sa_generated, payment_received, portal_opened, deliverable_uploaded, case_completed, final_reminder_sent, closed, and a handful more. Each row carries a timestamp, the actor (you, the client, the cron, or the AI), an IP address redacted to /24 (so the actor's network is identifiable but not their exact endpoint), and a JSON payload with the structured details. The ledger is INSERT-only at the database level: a Postgres trigger raises on any UPDATE attempt, even from the service role.

The audit-ledger card on the matter detail page renders the recent events in reverse chronological order with one line per event. Click any event to expand the JSON payload. The ledger is the canonical evidence of due-diligence and timing — when a Code review or a court asks who saw what and when, the ledger answers definitively. The data survives even when the underlying matter is deleted (we let parent rows cascade-delete to null on the ledger's foreign key so the audit history persists as orphans).

Notifications when the client acts

When the client takes a meaningful action — submits a fresh intake, returns through a continuation link, accepts or declines or asks to discuss a proposed price change, uploads new documents through the portal — the platform sends you a structured tenant-side notification email. The email is platform-branded (RCIC App via Investatech) so it stands out from your own tenant-branded sends, names the matter, summarizes the action, and links directly to the matter detail page on your dashboard. The reply-to is set to the client's email so a quick reply to the notification reaches them directly.

The notification recipient resolution defaults to the matter's responsible RCIC plus any Owner-configured Active File Review CC. When the responsible RCIC is unset (a brand-new intake that has not yet been assigned), the notification routes to the firm Owner. When an Accountant CC is configured for your firm, the accountant is CC'd on the bill-related notifications (Payment Request sent, payment received) but not on the workflow notifications (intake submitted, deliverable acknowledged, etc.) — the separation keeps your accountant's inbox focused on the financial-trail subset.

> **Note**: If you find yourself missing notifications, three things to check: (1) the matter has a responsible RCIC assigned (otherwise it routes to the Owner, who may not be the one who should see it), (2) you have not filtered out RCIC App via Investatech sender addresses in your inbox spam settings, (3) your firm has not silenced AFR notifications in Settings (we do not ship this kill switch in v1; you would have to manually mute the sender at your inbox level). If the AFR detail page shows a recent state change in its audit ledger but you never saw the notification, the most common cause is the second one above.

Integrations with other modules

AFR sits at the head of a multi-module workflow that the platform threads together via source pointers and back-link cards. The most important integration is the Service Agreements module: every generated SA carries a source pointer (source_kind = active_file_review, source_id = the AFR row id) so the SA detail page knows where it came from and can render a back-link card to the AFR detail. Conversely, the AFR detail's status pill mirrors the SA's lifecycle (SA generated -> SA sent -> SA signed) so you can track the SA's progress without bouncing between modules.

- Service Agreements: every AFR generates an SA. The SA's full lifecycle (validate, finalize, send, sign, counter-sign, fully-signed) lives in the SA module; the AFR mirrors high-level milestones via status transitions.
- Single Bills: the auto-bill that fires at fully-signed is a Single Bills row. Cancel-with-refund, manual mark-as-paid, and accountant CC all live on the Single Bills side; the AFR mirrors the Bill's paid / unpaid status on the pricing card.

- Transfer Room: when the SA reaches fully-signed, a Transfer Room is automatically provisioned for the matter (you can also activate it manually with a recorded reason). The seven-folder case tree provisioned by Transfer Room is the canonical operational workspace for the matter's ongoing file exchange; the Information Card on that Transfer Room is auto-filled from the AFR identity fields.
- AI Support: the AI extraction in this module shares the daily AI quota with the rest of the platform's AI surfaces (the in-dashboard AI Assistant, the booking-page AI document summary, the help-center chat). Premium tenants get the larger quota.

If you operate a multi-module workflow (intake form -> AFR -> SA -> Bill -> Transfer Room -> deliverable), the platform threads the same client identity across every module so you do not re-key client name, email, address, or matter context at any handoff. The AFR is where this thread starts for one-off response matters; for longer engagements (a full new-applicant retainer rather than a response to an existing one), an Intake Form or a Booking is often the better starting point.