



Deal review, buyer-side

Sample Co. booking platform

B2B appointment-booking SaaS for small clinics. About 140 paying customers, listed at £9,400 monthly recurring revenue. Under offer to a non-technical buyer.

Prepared for	Example Buyer Ltd (fictional)
Date	15 October 2026, version 1.0
Stack	Next.js, Supabase, Stripe, Vercel. Partly built with Cursor
Access used	Read-only: repository, Vercel, Supabase, Stripe, test account
Prepared by	Robert Udah, principal engineer, Holdfast

Sample report. The app, company and findings are invented to show the format.

Deal card

VERDICT

Fix, don't rebuild. About 18 hours before completion.

Proceed, on condition that findings 1 to 3 and 5 are fixed before completion and the former contractor signs an IP assignment.

Fix before completion

18 h

about £1,440

All findings

58 h

about £4,640 at £600 a day

Monthly revenue

£9,050

verified vs £9,400 listed (-3.7%)

Findings

14

2 critical, 3 high, 7 medium, 2 low

Key-person risk	High: the founder made 94% of commits and is the only person who has deployed
Open source	1 copyleft (AGPL) package in production; 3 packages with no declared licence
AI-generated code	About 55% of the code arrived in large single commits typical of AI tools; little sign of review
Contractor IP	One former contractor wrote 5% of commits; no IP assignment found
Cloud cost	£286 a month, £2.04 per customer (2.2% of revenue)
Hours include testing. Costs are estimates at a stated market rate, for negotiation, not quotes.	

Verdict

Fix, don't rebuild. About 18 hours before completion.

The data model is sound and the product works. The serious problems are a handful of configuration and access mistakes, not a rotten codebase. Two of them expose every customer's data today and must be fixed before money changes hands. The rest can follow in the first month of ownership.

What this means for the deal

Before completion

Ask the seller to fix findings 1 to 3 and move the accounts in finding 5 into the business's name. About 14 hours of work. If they won't, agree who pays for it.

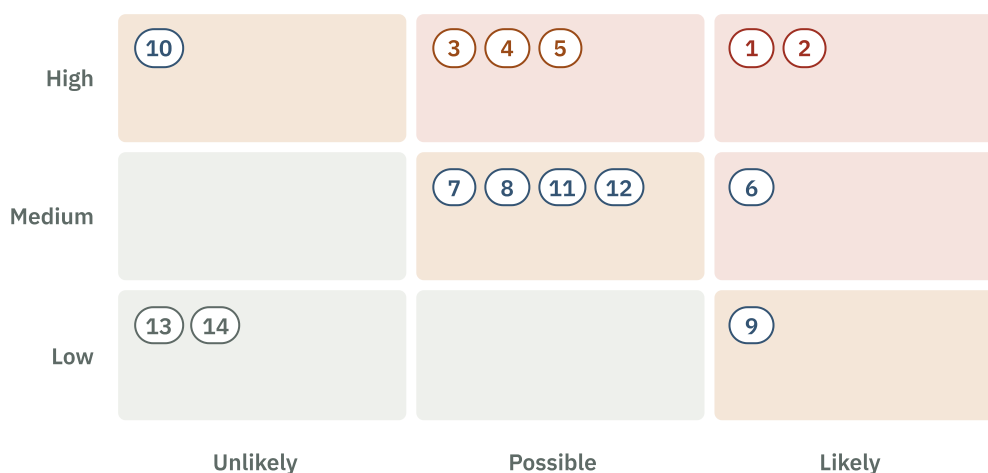
Revenue check

Stripe shows £9,050 a month, not the listed £9,400. Two annual plans were counted as monthly. Worth raising with the seller.

After close

Findings 4 and 6 to 12 fit into the first 90 days. None blocks the sale, but finding 6 is quietly leaking revenue and finding 10 needs a decision before you build on the code.

Risk map



Vertical: business impact. Horizontal: likelihood in the next 90 days.

Scorecard

1. Secrets and access	CRITICAL	8. Dependencies	MEDIUM
2. Authentication and authorisation	HIGH	9. Code health	MEDIUM
3. Data protection	CRITICAL	10. Data model	SOUND
4. Payments	HIGH	11. Open source and IP	MEDIUM
5. Backups and recovery	HIGH	12. AI features	MEDIUM
6. Hosting and deployment	HIGH	13. Cost and scalability	MEDIUM
7. Monitoring and operability	MEDIUM	14. Privacy and compliance	MEDIUM

Top findings

CRITICAL 1. Admin database key shipped to every browser

What	The Supabase service key, which bypasses all security rules, is included in the front-end code. Anyone who opens the site's developer tools can copy it.
Business risk	Anyone can read, change or delete every customer's data. A breach here is a reportable data incident.
Fix	Rotate the key today, move the two calls that use it to the server. About 3 hours (£240).
Confidence	Verified

CRITICAL 2. Customers can see other customers' bookings

What	Row-level security is switched off on 4 of 11 tables, including bookings and invoices. Changing one number in a request returned another clinic's records.
Business risk	Patient appointment data from one clinic is visible to others. Serious for trust and for UK GDPR.
Fix	Turn on and test rules for all 11 tables. About 6 hours (£480).
Confidence	Verified

HIGH 3. Payment webhook can be faked

What	The endpoint Stripe calls after a payment doesn't check the signature, so anyone can send a fake "paid" message.
Business risk	Accounts can be upgraded without paying. No sign it has been abused yet.
Fix	Verify signatures and ignore repeats. About 3 hours (£240).
Confidence	Verified

HIGH 4. Backups exist, restore never tested

What	Daily database backups are on, but nobody has ever restored one. Uploaded files (clinic logos, PDFs) aren't backed up at all.
Business risk	A bad migration or deletion could mean days of downtime, or permanent loss of uploaded files.
Fix	Test a restore on a copy, add storage backups, write a one-page recovery note. About 4 hours (£320).
Confidence	Evidence

HIGH 5. Key accounts belong to the founder personally

What	The domain, Vercel and Stripe accounts sit under the founder's personal email and card.
Business risk	If these don't transfer cleanly, the buyer doesn't fully own the business they paid for.
Fix	Move each into the company's name before completion. Plus the seller's time. About 2 hours (£160).
Confidence	Evidence

All findings

#	Finding	Area	Severity	Confidence	Hours	Cost
1	Service key in front-end bundle	Secrets	CRITICAL	Verified	3	£240
2	Row-level security off on 4 tables	Data protection	CRITICAL	Verified	6	£480
3	Webhook signature not verified	Payments	HIGH	Verified	3	£240
4	Restore untested, files not backed up	Backups	HIGH	Evidence	4	£320
5	Accounts in founder's personal name	Hosting	HIGH	Evidence	2	£160
6	Cancelled plans keep access for 30 days on 2 of 3 code paths	Code health	MEDIUM	Verified	10	£800
7	Framework two major versions behind; 3 high-severity package advisories	Dependencies	MEDIUM	Verified	4	£320
8	No tests on billing; error alerts go to an inbox nobody reads	Monitoring	MEDIUM	Verified	6	£480
9	No rate limiting or bot protection on sign-up	Authentication	MEDIUM	Verified	3	£240
10	AGPL-licensed PDF library used in the production server	Open source and IP	MEDIUM	Verified	6	£480

#	Finding	Area	Severity	Confidence	Hours	Cost
11	Clinic names and appointment times sent to an AI provider; no processor agreement on file	AI features	MEDIUM	Evidence	2	£160
12	Founder made 94% of commits; no written deploy or recovery steps	Operability	MEDIUM	Verified	4	£320
13	Missing security headers (CSP, HSTS) on the live site	Hosting	LOW	Verified	2	£160
14	README doesn't run; 14 unused routes	Code health	LOW	Verified	3	£240
Critical and high (before completion)					18	£1,440
All findings					58	£4,640

Confidence: **Verified** seen directly in code, configuration or a reproduced request. **Evidence** from exports or screenshots provided. **Reported** stated by the seller, not verified.

Open source and IP

882 packages in the software bill of materials. Licences are almost all permissive. One copyleft package needs a decision, and three have no declared licence.

Licences

Licence	Packages	Risk
MIT	612	Permissive
ISC	141	Permissive
Apache-2.0	88	Permissive
BSD-2/3-Clause	37	Permissive
AGPL-3.0	1	Copyleft: review
No declared licence	3	Unknown: review

Who wrote the code

Contributor	Commits	IP status
Founder	94%	Owner
Former contractor (2025)	5%	No IP assignment found
Automated dependency bot	1%	n/a

AI-generated code

About 55% of lines arrived in large single commits with the patterns typical of AI coding tools (Cursor, per the seller). Commit history shows little evidence of review. In some jurisdictions, code generated mainly by AI may not attract copyright protection, which can affect what is actually being bought.

For the buyer's lawyer

- Ask the seller for a signed IP assignment from the former contractor before completion.
- Ask whether the AI coding tool was used on a company or personal account, and under which terms.
- Decide whether to replace the AGPL PDF library (about 6 hours) or accept its obligations.

- Consider a specific warranty covering AI-generated code and third-party code in the SPA.

Holdfast does not give legal advice. These are technical facts and questions for your lawyer.

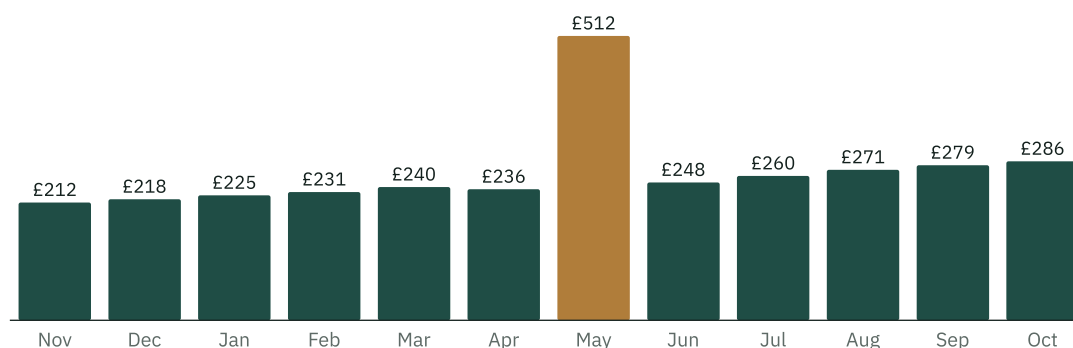
AI features

Drafts appointment reminder messages using a third-party AI model, called from the server.

Check	Result	Rating
Data sent to the provider	Clinic name, appointment time and the clinic's custom message. No patient names.	MEDIUM
Provider terms and processor agreement	API terms say inputs aren't used for training by default; no processor agreement on file; not listed in the privacy policy	MEDIUM
Prompt injection	Clinics can add custom text. Tested: it can change a clinic's own message, but cannot reach other clinics' data	SOUND
Isolation between customers	Each request carries only one clinic's data	SOUND
Cost	£18 a month, about £0.13 per customer	SOUND
Failure handling	If the provider is down, reminders silently fail; no retry or alert	MEDIUM

Cost and scalability

Monthly cloud and AI cost, last 12 months



The May spike (£512) was 41,000 fake sign-ups by bots over three days, which the seller couldn't explain. It's why finding 9 matters.

As the business grows

Customers	What happens	Monthly cost
Today (140 customers)	Comfortable	£286
2x (280 customers)	Fine. Booking search slows slightly	about £420
10x (1,400 customers)	Booking search does a full table scan; needs an index (2 hours) and a larger database tier	about £1,100

Live site

Mobile performance (Lighthouse)	61 / 100
Largest content visible (mobile)	3.8 s
Accessibility (Lighthouse)	78 / 100
Security headers (Observatory)	Grade D

Privacy and compliance

Check	Result	Detail
Privacy policy lists every processor	PARTLY	AI provider missing
Processor agreements on file	PARTLY	3 of 5
Where data is stored	NOTED	Database in the EU (Frankfurt); AI provider in the US
Cookie consent	FAIL	Analytics cookies set before consent
Retention and deletion	FAIL	No process to delete closed clinics' data
Accessibility basics	PARTLY	14 automated issues, mostly colour contrast

A technical check against UK GDPR basics, not a legal compliance opinion.

Transfer checklist

Every account the business depends on, and whether it moves cleanly to the buyer.

Account	Held by	Transfer route	Status
Domain	Founder, personal	Registrar account transfer	ACTION
Vercel hosting	Founder, personal	Move project to a company team	ACTION
Stripe	Founder, personal	Stripe account ownership change	ACTION
Supabase	Company organisation	Change organisation owner	READY
GitHub repository	Company organisation	Change organisation owner	READY
Email sending service	Company	Change account owner	READY
Analytics	Former contractor	Recreate under company	ACTION
Error tracking	Company	Change account owner	READY
SMS reminders API	Company	Check terms allow a change of owner	CHECK

Questions for the seller

Gaps only the seller can close. Ready to paste into the data-room request list.

1. Please provide a signed IP assignment from the 2025 contractor.
2. Which accounts (domain, hosting, Stripe, AI provider) are in your personal name, and will you transfer them before completion?
3. How many hours a week do you spend running the product, including support?
4. What caused the May cost spike, and has it happened before?
5. Have there been any security incidents, data breaches or customer complaints about data?
6. Which AI coding tools were used, and on which account?
7. Are there any customer contracts with custom terms, SLAs or data-location commitments?
8. Is any revenue from annual plans counted as monthly elsewhere in the listing?

Fix plan

1. **Before completion:** Rotate the leaked key and move it server-side (1), switch on row-level security (2), verify webhooks (3), move accounts into the company's name (5). Contractor IP assignment signed.
2. **First 30 days:** Test a restore and add file backups (4). Close the 30-day access gap (6). Add rate limiting to sign-up (9). Sign the AI provider's processor agreement and update the privacy policy (11).
3. **31 to 90 days:** Upgrade the framework and patch packages (7). Billing tests and working alerts (8). Replace or clear the AGPL library (10). Write deploy and recovery steps (12).
4. **91 to 180 days:** Security headers (13), clean-up (14), cookie consent and a data-deletion process. Add the booking index before growth demands it.

Method and evidence

Check	Tool	Headline result
Secrets in full git history	gitleaks	3 secrets found, 1 still live (finding 1)
Code vulnerability patterns	semgrep	27 results, 2 confirmed (findings 2, 3)
Known vulnerable packages	osv-scanner, npm audit	3 high-severity advisories (finding 7)
Software bill of materials and licences	syft, licence checker	882 packages; 1 AGPL, 3 undeclared (finding 10)
Code size and history	cloc, git log	38,400 lines (TypeScript, SQL); founder 94% of commits (finding 12)
Live site security	Mozilla Observatory	Grade D (finding 13)
Performance and accessibility	Lighthouse, axe	Mobile performance 61; 14 accessibility issues
Cost review	Provider billing exports	12 months reviewed; 1 unexplained spike, now explained

Full tool outputs are kept for 6 months and available on request.

Keeping it safe after the fixes

Monthly: patch dependencies, check that backups ran and a restore still works, review error alerts and uptime, and remove access for anyone who has left. About 2 to 4 hours a month for an app this size.

Holdfast Caretaker covers this routine for £750 a month, including up to four hours of fixes. Ask in the walkthrough call.

Scope and assumptions

Snapshot taken 13 October 2026 from the main branch and production configuration, with read-only access. Not included: penetration testing, load testing against production, legal or financial opinions. Hours assume a competent engineer new to the codebase and include testing; costs use £600 a day and are estimates. Severity and hours follow the Holdfast audit method: severity reflects what happens to the business if nobody acts.