

Production Readiness Review

QuoteYard

A fixed-price review of an app built on an AI app builder, before it takes real money from real customers. This is a sample, so you can see exactly what you get.

QuoteYard is a demo we built in-house on Lovable, the way a non-technical founder would, for the sole purpose of being reviewed here. No holes were planted and none were removed. Everything below is what the review actually found.

October 2026

Reviewed by Steve & Oliver Ford | steve@syriant.com

Built with Lovable (React, Supabase, Stripe) · Sample

■ The short version

Fix it, don't rebuild it.

QuoteYard is a careful build. The thing most AI-built apps get wrong, one business being able to read another's data, it gets right. Logins, data access and payments are handled properly. What's left is one unbuilt feature, three things worth hardening before real customers, and some polish. None of it is a reason to start again.

VERDICT

Fix, not rebuild

The foundation is sound. The work is finishing and hardening, not starting over.

SAFE TO TAKE REAL MONEY TODAY?

Not yet

Close. Fix the three medium items and send real emails first. Roughly a week of work.

3

Medium – fix
before launch

4

Low – fix soon

2

Worth knowing

0

Critical

Severity is about real customers and real money, not a checklist. "Medium" means fix it before you launch; "low" means soon after.

■ What we reviewed

- ✓ The code, as exported from the app builder, read end to end.
- ✓ How the database decides who can see what, every table and every rule.
- ✓ The logins, the invite and staff permissions, and the admin panel.
- ✓ The customer flow with no login: viewing a quote, accepting it, paying a deposit by card.
- ✓ The Stripe payment path and its webhook, and the AI that writes the quotes.
- ✓ Whether it scales: the database, the indexes, and what strains first under real traffic.
- ✓ A light accessibility pass on the pages your own customers see.
- ✓ The app builder's own security scans: what they caught, and what they missed.

US\$6,500 fixed, to fix what matters now

Covers the three medium findings, the unsent emails, and the two quick quality fixes (findings 1 to 4, 6 and 7). Paying each business directly through Stripe Connect (finding 5) is quoted separately, for when you scale. The US\$1,950 review fee is credited in full against fix work. GST is added for Australian clients.

■ What's already right

The hard parts are done properly.

We say this plainly because it's true, and because a review that only lists problems isn't telling you the whole picture. These are the things that most often go wrong in an AI-built app, and here they're handled the way they should be.

- ✓ **One business can't see another's data.** Every table has its access rules switched on, and each rule ties a row back to the business you belong to. This is the single biggest risk in apps like this, and it's covered.
- ✓ **The customer quote link is safe.** A customer opens their quote with a long, unguessable link and sees only their own quote. Logos and photos are served through short-lived private links, not left open to the web.
- ✓ **The deposit amount can't be tampered with.** It's worked out on the server from the quote, not taken from the customer's browser, and the payment is checked with Stripe before a quote is marked paid.
- ✓ **The admin panel can't be reached by an ordinary user.** Who is an admin is stored where a user can't change it, and every admin action checks it.
- ✓ **The free-plan limit can't be dodged.** The "3 quotes a month" cap is enforced in the database, so it holds even if someone pokes at the app from outside.
- ✓ **Deleting an account really deletes it.** It cancels billing, removes the files and photos, and removes the login, so a deleted account can't sign back in.

The app builder's own security scan was run too. It found and fixed one issue (business logos were readable by any signed-in user). It did not find any of the three on the next page.

■ Fix before launch

The three that matter.

MEDIUM

01 The browser decides whether a payment is real

What it is The app lets the customer's browser say whether a payment is in "test" mode or "live" mode, and the server believes it. On a live site that still has test keys set up, a customer could switch to test mode, pay the deposit with a well-known test card, and the quote would show as Paid, with no real money taken.

The fix Decide test-or-live on the server from the site's own settings, and ignore what the browser says. Small change, a few hours.

MEDIUM

02 Anyone with the link can accept, as anyone

What it is Whoever opens the quote link can accept it and type any name. There's no check that it's really the customer. In our test, one quote for "Darren Whitlock" was accepted under the name "Oliver Ford" and the app took it. For a document that triggers a card deposit and acts like an agreement, there's no proof of who actually said yes.

The fix Email the customer a one-time code to confirm before they accept or pay, and record the time it was accepted. About a day.

MEDIUM

03 Nothing slows down abuse, and the AI is a free tap

What it is The public pages (view, accept, pay) have no limit on how fast they can be hit, so a leaked link can be hammered. And the AI that writes quotes isn't counted against the free plan, so any free user can call it over and over and run up your AI bill.

The fix Add a simple rate limit to the public pages, and cap AI drafts per business per day. About a day.

■ Fix soon

Smaller things, and two to know about.

LOW

04 The app doesn't actually send email

What it is "Send to customer" and the staff invite open your own email program with the link pasted in. On a laptop, nothing opened at all. The app doesn't send anything itself, so a core step is manual.

The fix Send email from the app through a proper sending service, from an address on a domain you own. Needed before any real launch. About a day, including the domain set-up.

LOW

05 Every business shares one payment account

What it is All deposits go into a single Stripe account, and every customer sees the same name at checkout, not the tradie's own business. Fine for now, but it means the money doesn't reach each business directly.

The fix Move to Stripe Connect so each business is paid into its own account. A larger piece, best done when you're ready to scale. Quoted separately.

LOW

06 Business details aren't checked, and reach the PDF raw

What it is ABNs are accepted even when they're not valid. In testing, a business name was saved as a stray computer file path and then printed straight onto the customer's quote and PDF, overlapping the other text. Whatever is typed reaches the customer as-is.

The fix Check the ABN, tidy and bound the business name, and clean the fields before they go on a customer document. A few hours.

LOW

07 The PDF is heavy and leaves out the photos

What it is A one-page quote PDF comes out around 6 MB, and the job photos aren't on it. It's made in the browser, which is why it's large.

The fix Shrink the logo and build the PDF on the server, and include the photos. A few hours.

WORTH KNOWING 08

The payment safety-check is slightly loose

One part of the webhook check compares values in a way that isn't the strict, timing-safe method. The secret still protects it, so the real-world risk is tiny. Worth tightening when you're in there.

WORTH KNOWING 09

Errors are sent to the app builder

When something breaks, the details are sent to Lovable's error service. Before you have real customer data, check what's included so nothing sensitive leaves with it.

■ Will it scale?

Yes, with a few tweaks.

It's built to grow to the customers you're chasing, thousands of small trade businesses, without hitting a wall. The groundwork is right; a handful of things would slow down only once you're busy.

Holds up

- ✓ Every busy database lookup is indexed by business, so it stays fast as the data grows.
- ✓ Quote numbering can't collide, even with lots of people saving at once.
- ✓ The free-plan limit is enforced in the database, not the browser.

Watch as you grow

- ✓ The admin page counts every quote for every business at once. Fine at dozens, slow at thousands.
- ✓ No rate limiting, which is a load problem as well as an abuse one (finding 3).
- ✓ The PDF is built in the browser at 6 MB (finding 7), and a fresh link is made for every photo on every view.
- ✓ Database connection pooling is the first thing we'd confirm under real traffic.

■ Can everyone use it?

A good start, a few fixes.

A light accessibility pass, weighted to the public quote page, since that's where your customer, who might be an older homeowner, actually views, accepts and pays.

Already right

- ✓ Built on accessible building blocks, with the page language set.
- ✓ Images carry text descriptions for screen readers.
- ✓ The accept and decline forms have proper labels.

To fix

- ✓ Some secondary text is small and light grey. Check it meets the readable-contrast minimum.
- ✓ The in-app photo viewer can't be closed with the keyboard, only the back button.
- ✓ Success and error messages may not be announced to screen-reader users.

This is a readiness pass, not an ADA or WCAG compliance certificate. A full accessibility audit, with a keyboard-only and screen-reader walkthrough of the whole customer journey, is a separate piece if you need to prove compliance.

■ Fix or rebuild, with the numbers

Fixing is far cheaper than starting again.

PATH	WHAT IT TAKES	ROUGH COST
Fix what matters now Findings 1 to 4, 6, 7	About 3 to 4 days. Payment mode, acceptance by code, rate limits and AI cap, real emails, input checks, the PDF.	US\$6,500
Pay each business directly Finding 5, Stripe Connect	A larger piece, for when you take on real volume. Scoped separately.	From US\$4,000
Rebuild from scratch	Throw away a sound, working app and its data model. Weeks, not days, and you'd most likely rebuild the same thing.	US\$28,000+

The US\$1,950 review fee is credited in full against fix work, whatever its size. GST is added for Australian clients.

■ What we'd confirm in your live app

A review reads the code; a few things we'd also check running, and would in a real engagement:

- ✓ Sign in as one business and try to open another's quote by its address. The rules say it's blocked; we'd prove it.
- ✓ Whether the Pay button still shows after a deposit is paid, so nobody pays twice.
- ✓ Google sign-in, which hasn't been tested, and that the dashboard figures match the real data.

This is what every review looks like.

Steve & Oliver Ford

steve@syriant.com

syriant.com

A real review comes with a recorded walkthrough showing each finding in your own app, and we take you through it on a call if you want. Yours in 48 hours from read-only access.