

Folioport payments and apps: what was found and what was fixed

Prepared for: Folioport's founder (a fictional client portal for design studios)

Prepared by: Ilya Shkura

The app: React and TypeScript on Firebase; Stripe on the website; Android and iPhone apps from the same code (Capacitor); in-app purchases through RevenueCat, added in the fixes

FOUND

25

7 high, 7 medium, 11 low

FIXED AFTER THREE
ROUNDS

22

of 25; 2 in part, 1 left to the founder

HIGH OPEN AFTER THE
LAST ROUND

2

brought by the last fixes;
listed below

Summary for the founder

Paying for a plan worked on the normal path, on the website and in the Android app, but the money stopped following the founder's rules as soon as anything unusual happened. Studios already on paid plans kept them for nothing, a studio bigger than Free could not cancel, a handover left the previous owner's card paying, a plan given free of charge went on charging, the apps sold plans in a way the stores refuse, and clients could not sign in to the app at all. After three rounds of fixes 22 of the 25 are fixed, 2 high ones in part and 1 is left to the founder. The in-app purchases added in the fixes brought four high problems of their own, fixed in the third round; the checks after that last round found two new high ones, listed below and left open.

FOUND

25

7 high, 7 medium, 11 low

FIXED

22 of 25

2 in part, 1 left to the founder

As received: "Payments work on the emulator against your Stripe test account, and there's a working Android app that I tested on the Pixel 7 emulator. That includes a studio owner paying for a plan inside the app. ... Cancelling is always allowed, even if the studio is bigger than Free allows."

What was fine: Buying, renewing, a trial without a card, a failed payment retried and then ended, cancelling to the end of the month, moving up and a partial refund did what the founder's table says; only the owner could pay; the founder's other businesses at Stripe were left alone; nothing was ever deleted when a plan ended.

What mattered most

HIGH

Studios already on a paid plan kept it for nothing

Agency for nothing, with no end; €79 a month in the founder's revenue

HIGH

An owner whose studio is bigger than Free could not cancel

"Cancel and move to Free" greyed out: "Remove some on the Team page first"

HIGH

After a handover the previous owner's card kept paying

Agency billed to the previous owner's card (next invoice €129); they can't cancel

HIGH

A plan given free of charge kept charging the card

€29 charged again a month later; the owner reads "Contact us to change it"

HIGH

Clients could not sign in to the app at all

Signed in in the browser; the app still on "Check your inbox"

HIGH

The apps sold plans in a way the stores refuse

Stripe's page, €29 by card, in a build for every country

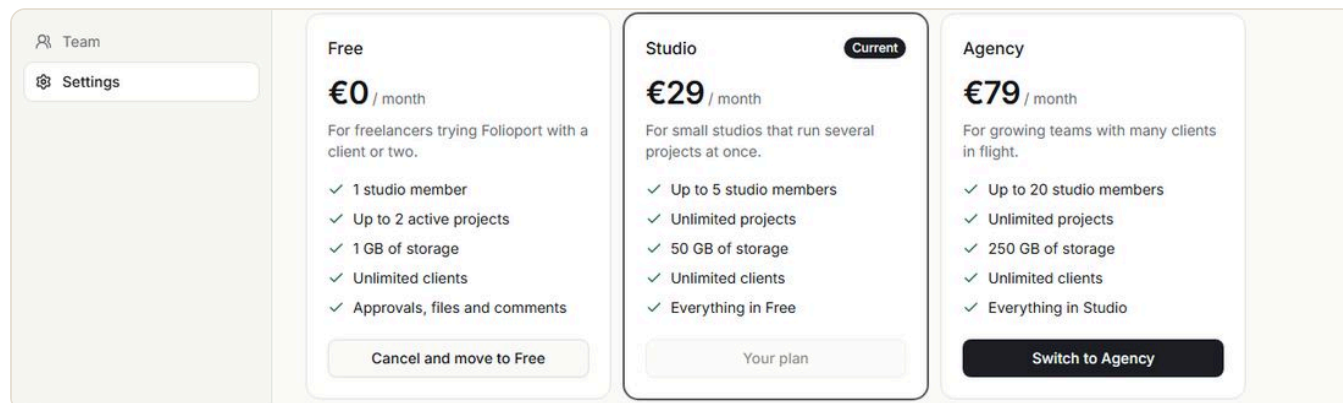
HIGH

The store build without payments still asked people to buy

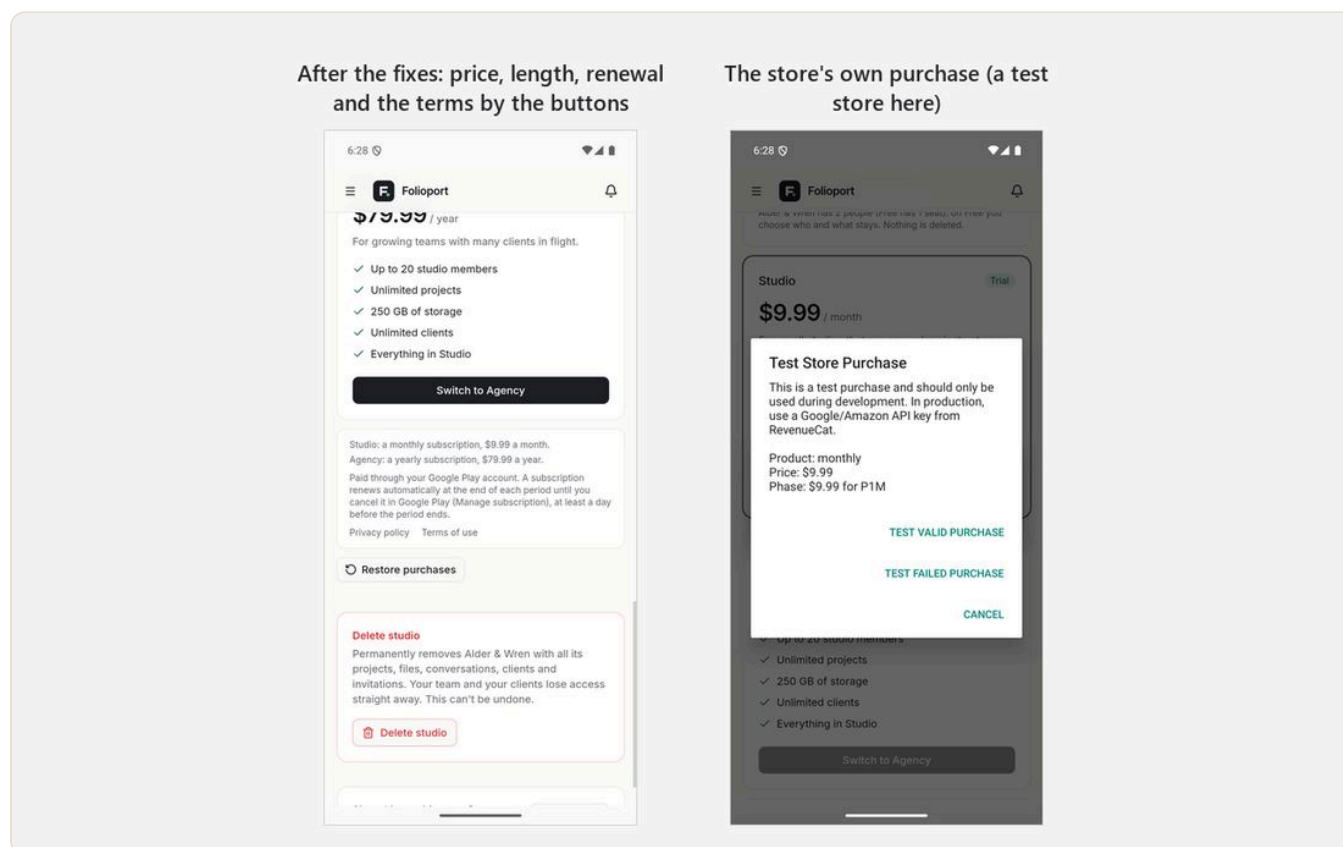
"See plans", "Upgrade", "Choose a plan"; tapped: "The plan can't be changed in this app"

Folioport

A portal where design studios share work with their clients: projects with stages, client approvals, files, conversations and plans with limits. In this case the builder added paying for the Studio and Agency plans with Stripe on the website, Android and iPhone apps, and, during the fixes, Apple's and Google's in-app purchases. Built with Claude Code from plain-language messages.



The website: plans paid through Stripe, and the way to cancel



The Android app after the fixes: the store's own purchase, with the terms by the buttons

All findings

#	SEVERITY	FINDING	AREA	AFFECTS	STATUS
1	HIGH	Studios already on a paid plan kept it for nothing	Money	Founder	Fixed
2	HIGH	An owner whose studio is bigger than Free could not cancel	Money	Studio owners	Fixed
3	HIGH	After a handover the previous owner's card kept paying	Money	Studio owners	Partly
4	HIGH	A plan given free of charge kept charging the card	Money	Studio owners	Fixed
5	HIGH	Clients could not sign in to the app at all	Mobile	Clients and studios	Partly
6	HIGH	The apps sold plans in a way the stores refuse	Mobile	Founder	Fixed
7	HIGH	The store build without payments still asked people to buy	Mobile	Founder	Fixed
8	MEDIUM	Two payment pages could make two subscriptions	Money	Studio owners	Fixed
9	MEDIUM	A suspended studio was charged and could not cancel	Money	Studio owners	Fixed
10	MEDIUM	A Stripe message was lost if handling it failed once	Money	Founder and studio owners	Fixed
11	MEDIUM	A studio deletion that stopped halfway kept charging	Money	Studio owners	Fixed
12	MEDIUM	Taking a photo would have closed the iPhone app	Mobile	Everyone on iPhone	Fixed
13	MEDIUM	Saving a big file gave an empty file without an error	Mobile	Everyone in the apps	Fixed
14	MEDIUM	The store build told owners to update their card outside the app	Mobile	Founder	Fixed
15	LOW	The founder's revenue came from plan names, not payments	Money	Founder	Fixed
16	LOW	One purchase showed twice in the studio's history	Money	Founder	Fixed
17	LOW	Late Stripe messages left records under a deleted studio	Money	Founder	Fixed
18	LOW	No email when a plan is paid or a payment fails	Money	Studio owners	Left
19	LOW	"Open in Stripe" always opened test mode	Money	Founder	Fixed
20	LOW	Members saw plan prices meant for the owner	Access	Studio	Fixed
21	LOW	The Android upload had no camera	Mobile	Everyone on Android	Fixed
22	LOW	With no connection the app showed misleading screens	Mobile	Everyone in the apps	Fixed
23	LOW	Back from a full-screen file left the project	Mobile	Everyone on Android	Fixed
24	LOW	Website links could never open the iPhone app	Mobile	Founder	Fixed

25	LOW	The live site accepted any localhost address to return to after paying	Money	Studio owners	Fixed
----	-----	--	-------	---------------	-------

1 HIGH Studios already on a paid plan kept it for nothing

Studios that were on Studio or Agency before payments existed stayed on them with no subscription, and nothing ever asked them to pay. The founder's revenue counted them as paying, at the plan's price.

Atelier Brume, on Agency since before payments

AS RECEIVED

Agency for nothing, with no end; €79 a month in the founder's revenue

AFTER THE FIX

"The Agency plan isn't paid for yet": pay by the date or move to Free; revenue €0

HOW TO REPRODUCE

1. Take a studio that was on Studio or Agency before payments existed.
2. Open its Settings and the founder's revenue.

THE FIX

Paid plans nobody pays for get 14 days' notice, like a trial ending: the owner can keep the plan by paying, and after the date the studio moves to Free under the usual over-limit rules. Revenue counts them as €0.

Check: opened studios that were on paid plans before payments, moved time on past the notice and read the founder's revenue. **Fixed.** Money · affects: Founder

2 **HIGH** An owner whose studio is bigger than Free could not cancel

An owner with more people than Free allows could not stop paying: "Cancel and move to Free" was greyed out, and Stripe's own page had no cancel either. The only way out was to remove people first.

The owner of a paying Studio with 2 people wants to stop paying

AS RECEIVED

"Cancel and move to Free" greyed out: "Remove some on the Team page first"

AFTER THE FIX

Cancel works; Studio runs to the end of the paid month, then Free, nothing deleted

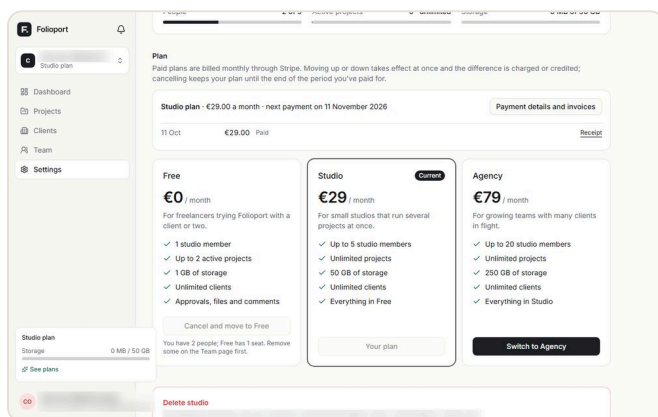
HOW TO REPRODUCE

1. Pay for Studio and add a second person.
2. Open Settings, Plan, and try "Cancel and move to Free", or cancel on Stripe's page.

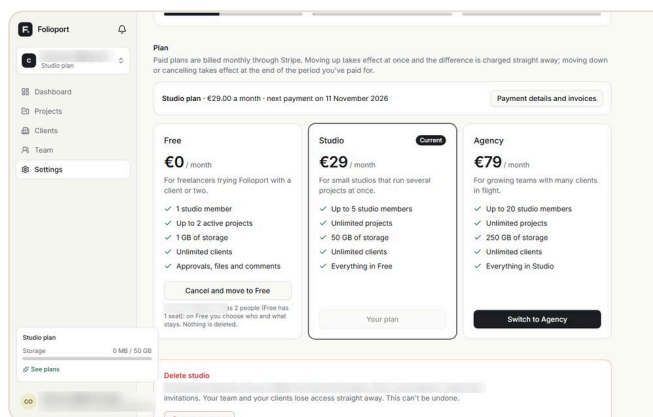
THE FIX

Cancelling and moving down are always allowed, whatever the studio's size; they take effect at the end of the paid period, and nothing is deleted.

Check: as the owner of a paying studio with two people, cancelled from Settings and on Stripe's page. **Fixed**. Money · affects: Studio owners



AS RECEIVED



AFTER THE FIX

3 **HIGH** After a handover the previous owner's card kept paying

When an owner handed the studio over, the subscription stayed on the previous owner's card. The new owner could move up and the old card paid for it, and the previous owner, now only a member, could no longer cancel.

A paying studio handed to a member, who then moves up to Agency

AS RECEIVED

Agency billed to the previous owner's card (next invoice €129); they can't cancel

AFTER THE FIX

The previous owner's subscription ends with its paid month; the new owner pays with their own card

HOW TO REPRODUCE

1. Pay for Studio as the owner.
2. Hand the studio over to a member.
3. As the new owner, switch to Agency; as the previous owner, try to cancel.

THE FIX

Each owner pays as their own Stripe customer. After a handover the previous owner's subscription runs to the end of its paid month and is never charged again; the new owner pays from then on, at once for a bigger plan, and sees only their own payments.

Check: handed a paying studio to a member, moved up as the new owner and tried to cancel as the previous one. **Partly fixed:** For studios whose payment was set up on the version as handed over, two gaps remain after the last round: once the new owner opens their own payment page, the month the previous owner already paid for is charged again; and until such a studio's billing is checked once, the new owner can still see the previous owner's payments and open their card page (read from the code). Money · affects: Studio owners

4 HIGH A plan given free of charge kept charging the card

When the founder gave a paying studio a plan free of charge, its Stripe subscription went on charging the card every month. The owner was told to contact the founder and had no way to cancel, and the founder's revenue showed €0 while the money came in.

Agency given free of charge to a studio paying €29 for Studio

AS RECEIVED

€29 charged again a month later; the owner reads "Contact us to change it"

AFTER THE FIX

Subscription cancelled at once, €28.99 of unused time refunded, no more charges

HOW TO REPRODUCE

1. Pay for Studio.
2. As the founder, give the studio Agency free of charge.
3. Wait for the next renewal.

THE FIX

Giving a paying studio a plan free of charge cancels its subscription at once and refunds the unused part of the month. The founder can't change a paying studio's plan any other way.

Check: gave Agency free of charge to a studio paying for Studio and moved time on a month. **Fixed.** Money · affects: Studio owners

5 **HIGH** Clients could not sign in to the app at all

The sign-in link from the email opened the phone's browser and signed the person in on the website, while the app stayed on "Check your inbox". Clients sign in only with these links, so a client could not get into the app; invitations worked the same way.

A client asks for a sign-in link in the Android app

AS RECEIVED

Signed in in the browser; the app still on "Check your inbox"

AFTER THE FIX

The link opens the app and the client is in, in about 9 seconds

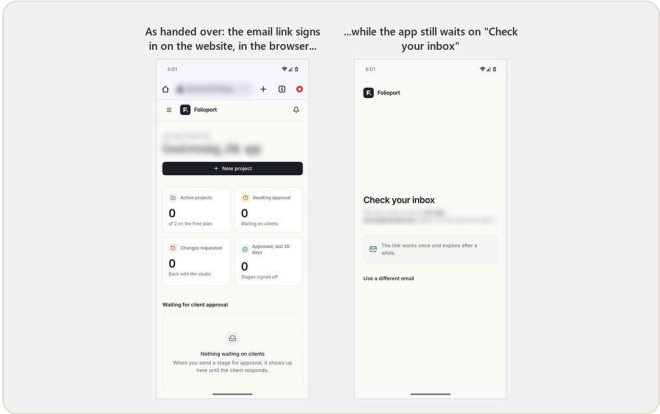
HOW TO REPRODUCE

- 1. In the app, tap "Sign in with an email link instead".
- 2. Open the link from the email on the phone.

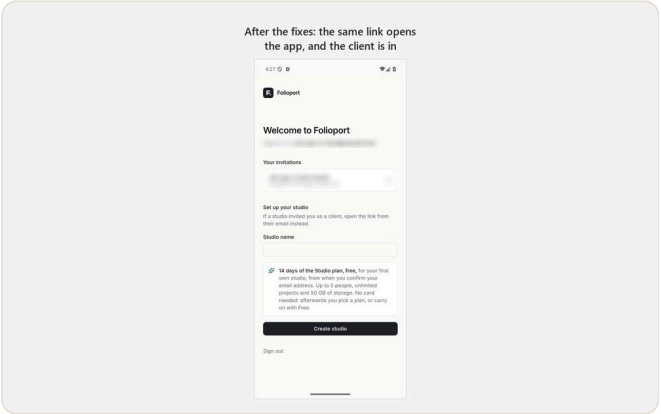
THE FIX

The email link opens a small page that hands the sign-in over to the app, with signing in in the browser as the fallback; invitations work the same way. Checked on Android; the iPhone side from the project.

Check: asked for sign-in links in the Android app and opened them as from the email: a client's sign-in, a client's invitation and a member's invitation. **Partly fixed:** Read from the code after the last round: a store build set up as the notes say sends the email's link through Firebase's default address, which may open the browser again, and pointing the emails at the website would make the app catch email confirmation and password reset links it can't handle. The iPhone app wasn't built. Mobile affects: Clients and studios



AS RECEIVED



AFTER THE FIX

6 HIGH The apps sold plans in a way the stores refuse

The apps had no Apple or Google in-app purchase: an owner paid in the app on Stripe's page, and one build was meant for every country. Google Play doesn't allow selling a subscription that way, and Apple allows it only on the US App Store, so the apps would be refused.

A studio owner pays for Studio in the Android app

AS RECEIVED

Stripe's page, €29 by card, in a build for every country

AFTER THE FIX

The store's own purchase (tried with a test store); the website shows where the plan is paid

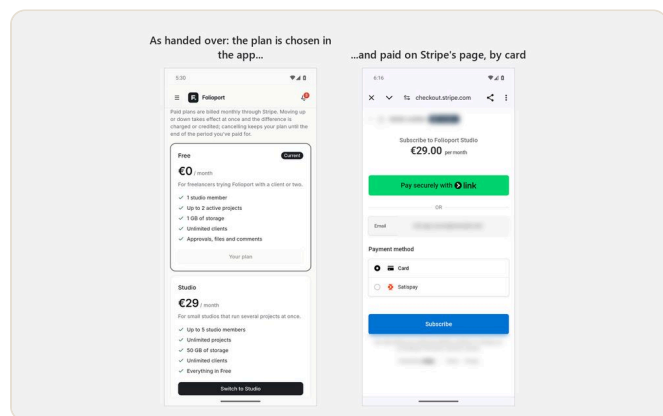
HOW TO REPRODUCE

1. Open the app as a studio owner and choose a paid plan.
2. See where the payment happens.

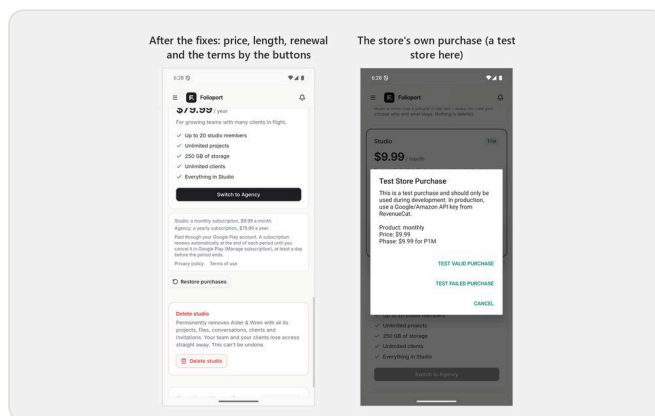
THE FIX

Studio and Agency are bought in the apps through Apple's and Google's own purchases, with Restore and the store's subscription page. A plan paid on the website isn't offered again in the app, and a plan bought in the app can't be changed on the website. The US-only variant shows its links to the website only to people in the US App Store.

Check: looked for the stores' purchases in the build and paid for a plan in the Android app; after the fixes, bought, moved up and down and restored purchases with a test store. **Fixed.** Mobile · affects: Founder



AS RECEIVED



AFTER THE FIX

7 **HIGH** The store build without payments still asked people to buy

The build meant for the stores, with payments switched off, still showed "See plans", "Upgrade for more", "Choose a plan" and the prompts at a plan's limit, all ending at "The plan can't be changed in this app". Apple rejects an app that points people to buying a plan it doesn't sell itself.

Studio Halden at its project limit, in the build without payments

AS RECEIVED

"See plans", "Upgrade", "Choose a plan"; tapped: "The plan can't be changed in this app"

AFTER THE FIX

No buying prompts; in the build with in-app purchases they lead to the store

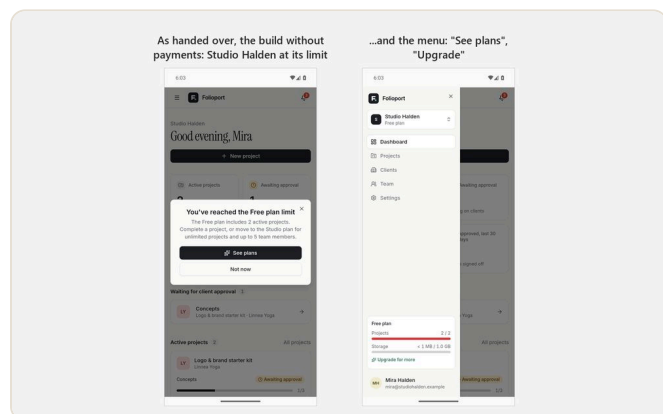
HOW TO REPRODUCE

1. Make the store build without payments.
2. Open a Free studio at its limit: dashboard, menu, New project, Team, Settings.

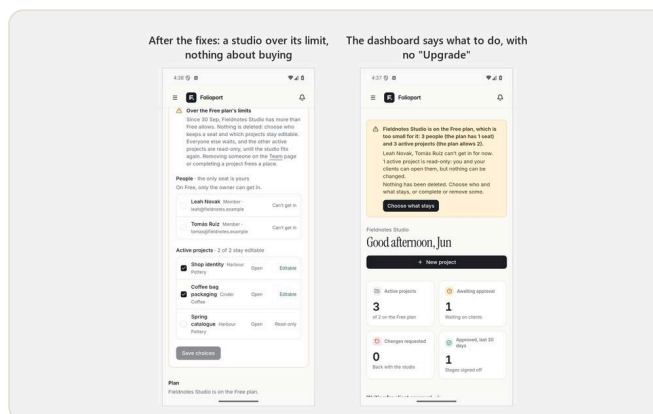
THE FIX

In a build without payments nothing mentions buying; in a build with in-app purchases these prompts lead to the store purchase.

Check: opened the store build without payments as a studio at its limit, over its limit and with an unpaid plan; the same code runs on iPhone. **Fixed**. Mobile · affects: Founder



AS RECEIVED



AFTER THE FIX

The other findings

8 **MEDIUM** Two payment pages could make two subscriptions

WHAT HAPPENS

A payment page opened on the website and another opened in the app could both be paid. The studio then had two subscriptions charging every month, the plan followed the one paid last, and cancelling stopped only one of them.

HOW TO REPRODUCE

1. Open the payment page for Agency on the website.
2. Open the payment page for Studio in the app.
3. Pay both, then cancel.

Agency paid on the website and Studio in the app, both pages opened first

AS RECEIVED

€79 + €29 every month; the plan shows Studio; a cancel stops only Studio

AFTER THE FIX

A new page closes the old one; if both are paid, Agency stays and Studio is refunded €28.99

THE FIX

Opening a new payment page closes the earlier one. If two payments still go through, the bigger plan stays, the other is cancelled with its unused part refunded, and the owner is told in Settings.

Check: opened two payment pages before either was paid, paid both and cancelled. **Fixed.** Money - affects: Studio owners

9 **MEDIUM** A suspended studio was charged and could not cancel

WHAT HAPPENS

A suspended studio kept being charged, and its owner could neither cancel nor open the payment page: both were refused with "This studio is suspended". The owner paid for a studio they couldn't use.

HOW TO REPRODUCE

1. Pay for Studio.
2. As the founder, suspend the studio.
3. As the owner, try to cancel; wait for the renewal.

A studio on Studio, suspended by the founder

AS RECEIVED

€29 charged during the suspension; cancel refused

AFTER THE FIX

Nothing collected while suspended; the owner can cancel

THE FIX

Nothing is collected while a studio is suspended, and its owner can still cancel and open the payment page. Lifting the suspension asks for the current month to be paid, with the usual notice.

Check: suspended a paying studio, moved time on through a renewal and tried to cancel as its owner. **Fixed.** Money - affects: Studio owners

10 **MEDIUM** A Stripe message was lost if handling it failed once

WHAT HAPPENS

If handling a message from Stripe failed once, Stripe's retry was taken for a repeat and dropped. A lost message about a cancelled or failed payment leaves the plan as it was, without the money behind it.

HOW TO REPRODUCE

1. Make the handling of one Stripe message fail once.
2. Let Stripe send it again.

A Stripe message whose handling fails the first time

AS RECEIVED

The retry answered "duplicate": the change never applied

AFTER THE FIX

The retry is handled; only the next copy counts as a repeat

THE FIX

A Stripe message counts as handled only once everything for it is done, so Stripe's retry finishes the job; a failed look-up of the customer also lets Stripe retry.

Check: made the handling of one Stripe message fail once, then let Stripe deliver it again. **Fixed**. Money · affects: Founder and studio owners

11 **MEDIUM** A studio deletion that stopped halfway kept charging

WHAT HAPPENS

Deleting a studio cancelled its subscription only at the very end. If the deletion stopped after its first step, the studio showed as "Being deleted" while the card was still charged every month.

HOW TO REPRODUCE

1. Start deleting a paying studio and let it stop after the first step.
2. Wait a month.

A paying studio's deletion stops after its first step

AS RECEIVED

A month later: subscription active, €29 charged

AFTER THE FIX

Subscription stopped at the first step; nothing charged a month later

THE FIX

The first step of deleting a studio stops its subscription, and a regular clean-up stops any that are left.

Check: stopped a studio's deletion after its first step and moved time on a month. **Fixed**. Money · affects: Studio owners

12 **MEDIUM** Taking a photo would have closed the iPhone app

WHAT HAPPENS

The iPhone project didn't say why the app needs the camera and photos. The upload offers "Take Photo" on iPhone, and choosing it without that explanation makes iOS close the app; Apple's review checks it too.

HOW TO REPRODUCE

1. Open a project in the iPhone app and add a file.
2. Choose "Take Photo".

Someone taps "Take Photo" to upload, on iPhone

AS RECEIVED

No reason given for the camera: iOS closes the app

AFTER THE FIX

The app says why it needs the camera and photos

THE FIX

The iPhone project says why the app needs the camera, the photo library and the microphone.

Check: read the iPhone project's settings for the camera and photos. **Fixed**. Mobile · affects: Everyone on iPhone

13 **MEDIUM** Saving a big file gave an empty file without an error

WHAT HAPPENS

Saving a file in the app read the whole file into memory at once. In a check of that step 100 MB came through but 420 MB came back empty, so the phone would have saved an empty file without a word, though the portal allows files up to 500 MB.

HOW TO REPRODUCE

1. Open a file of a few hundred MB in the app.
2. Save it to the phone.

Saving a 420 MB file in the app

AS RECEIVED

An empty file, no error

AFTER THE FIX

A 300 MB file saved whole; a cut connection says so and saves nothing

THE FIX

Files are written to the phone as they arrive and checked for size; if the whole file doesn't arrive, nothing is saved and the app says so. Zips of unknown size are checked for being complete.

Check: saved large files in the Android app and cut the connection halfway. **Fixed.** Mobile · affects: Everyone in the apps

14 **MEDIUM** The store build told owners to update their card outside the app

WHAT HAPPENS

In the store build without payments, after a failed renewal the owner read "update your card to keep the Studio plan"; with no way to do it in the app. That points people to managing payment outside the app, which Apple doesn't allow.

HOW TO REPRODUCE

1. Make the store build without payments.
2. Let a renewal fail and open the app as the owner.

A failed renewal, in the store build without payments

AS RECEIVED

"Stripe will try again; update your card to keep the Studio plan."

AFTER THE FIX

"Your last payment didn't go through. Stripe will try again."

THE FIX

The store build without payments says only that the last payment didn't go through and Stripe will try again.

Check: showed a failed renewal in the store build without payments; the same code runs on iPhone. **Fixed.** Mobile · affects: Founder

15 **LOW** The founder's revenue came from plan names, not payments

WHAT HAPPENS

The monthly revenue was worked out from each studio's plan, not from what was paid, so it counted studios that paid nothing and missed money that came in. The builder had listed this as not done.

HOW TO REPRODUCE

1. Buy during a trial, refund a payment in full, or pay twice.
2. Open the founder's revenue.

The founder's revenue for unusual studios

AS RECEIVED

Trial days: €29; refunded in full: €29; two subscriptions (€108 charged): €29

AFTER THE FIX

What Stripe charged in the last 30 days minus refunds

THE FIX

Revenue comes from what Stripe charged in the last 30 days minus refunds and disputed payments, in total and per studio, plus what the stores report.

Check: compared the founder's revenue with what Stripe charged, for a purchase in a trial, a full refund, two subscriptions and a plan free of charge. **Fixed.** Money · affects: Founder

16 LOW One purchase showed twice in the studio's history

WHAT HAPPENS

When Stripe delivered a purchase's messages at the same moment, the studio's history recorded the same plan change twice.

HOW TO REPRODUCE

1. Buy a plan.
2. Let Stripe deliver its messages at the same moment.

One purchase, its Stripe messages arriving together

AS RECEIVED

Two "free → studio" lines

AFTER THE FIX

One line

THE FIX

Simultaneous Stripe messages write the history once.

Check: delivered a purchase's Stripe messages at the same moment.

Fixed. Money · affects: Founder

17 LOW Late Stripe messages left records under a deleted studio

WHAT HAPPENS

Messages from Stripe that arrived after a studio was deleted left new records under it, which nobody could see or clean up.

HOW TO REPRODUCE

1. Delete a paying studio.
2. Let Stripe deliver a late message about it.

A late Stripe message about a deleted studio

AS RECEIVED

New records under the deleted studio

AFTER THE FIX

Acknowledged, nothing written

THE FIX

A message about a studio that's gone is acknowledged and nothing is written.

Check: sent Stripe messages about deleted studios. **Fixed.** Money · affects: Founder

18 LOW No email when a plan is paid or a payment fails

WHAT HAPPENS

Owners got no email when they paid or when a payment failed, and the setup notes didn't say which Stripe settings would send them. A failed payment showed only as a notice in the app.

HOW TO REPRODUCE

1. Pay for a plan, or let a renewal fail.
2. Look for an email.

An owner pays, or a renewal fails

AS RECEIVED

No email, and no word on Stripe's own emails

LEFT AS IT IS

Still no email from the portal; Stripe's switches for receipts and failed payments named for the founder

LEFT TO THE FOUNDER

No emails were built. The builder named Stripe's own switches for receipts, refunds and failed payments; they apply to the whole Stripe account the founder shares with other businesses, so switching them on is the founder's call.

Check: looked for receipts and failed-payment emails from the portal and in its setup notes. **Left to the founder.** Money · affects: Studio owners

19 **LOW** "Open in Stripe" always opened test mode

WHAT HAPPENS

The founder's "Open in Stripe" link always pointed at Stripe's test mode, so with a live key it would not show the customer.

HOW TO REPRODUCE

1. Run the portal with a live Stripe key.
2. Open a studio in the founder's admin and click "Open in Stripe".

"Open in Stripe" on a studio's page, with a live key

AS RECEIVED

Opens test mode

AFTER THE FIX

Opens test or live mode to match the key

THE FIX

The link opens test or live mode to match the key in use.

Check: followed the link with the test key; the live-key case read from the code. **Fixed**. Money · affects: Founder

20 **LOW** Members saw plan prices meant for the owner

WHAT HAPPENS

Settings is open to the whole team, and a member saw the plan cards with prices and greyed-out switch buttons, on the website and in the app. Only the owner should see prices and plan buttons.

HOW TO REPRODUCE

1. Sign in as a member of a paying studio.
2. Open Settings.

A member of Atelier Brume opens Settings

AS RECEIVED

Cards €0 / €29 / €79 and "Switch to Free / Studio"

AFTER THE FIX

"...is on the Agency plan. Only the owner can change the plan."

THE FIX

Members see which plan the studio is on, without plan cards or prices.

Check: opened Settings as a member on the website and in the Android app. **Fixed**. Access · affects: Studio

21 **LOW** The Android upload had no camera

WHAT HAPPENS

On Android the upload picker offered images, documents and Drive, but no camera, so nobody could take a photo and send it.

HOW TO REPRODUCE

1. Open a project in the Android app.
2. Start an upload.

A client starts an upload on Android

AS RECEIVED

Picker without a camera

AFTER THE FIX

"Take a photo" opens the camera; the photo lands in the project

THE FIX

A "Take a photo" button opens the phone's camera and the photo is uploaded like any file. The first attempt still opened the picker; the second round fixed it.

Check: started an upload as a client and as a member on Android, then took a photo. **Fixed**. Mobile · affects: Everyone on Android

22 LOW With no connection the app showed misleading screens

WHAT HAPPENS

With no connection the app showed screens that looked like real answers: a client saw "No active projects", or "Set up your studio" when starting the app. Nothing said the phone was offline.

HOW TO REPRODUCE

1. Turn off Wi-Fi and mobile data.
2. Open the app.

A Studio Halden client opens the app with no connection

AS RECEIVED

"No active projects. Studio Halden will add your projects here."

AFTER THE FIX

"No connection", gone by itself when the connection returns

THE FIX

A "No connection" screen covers the app while offline and goes away by itself.

Check: turned Wi-Fi and mobile data off with the app open and before starting it. **Fixed**. Mobile · affects: Everyone in the apps

23 LOW Back from a full-screen file left the project

WHAT HAPPENS

Back from a file shown full screen left the project for the portal's list, instead of closing the file.

HOW TO REPRODUCE

1. Open a file full screen in a project.
2. Press Back.

Back from a file shown full screen

AS RECEIVED

Out of the project, on the portal's list

AFTER THE FIX

File closed, still in the project

THE FIX

Back closes a file shown full screen, then any dialog, before leaving the page.

Check: opened a file full screen in a project and pressed Back. **Fixed**. Mobile · affects: Everyone on Android

24 LOW Website links could never open the iPhone app

WHAT HAPPENS

In the iPhone project the file that lets website links open the app wasn't attached to the app, and Apple's team id was a placeholder, so website links would never have opened the iPhone app.

HOW TO REPRODUCE

1. Open the iPhone project's build settings.
2. Look for the website-links file and the team id.

The iPhone build's website-links setting

AS RECEIVED

Not attached; team id a placeholder

AFTER THE FIX

Attached to every build; the team id in one place for the founder

THE FIX

The website-links file is part of the iPhone build, and the Apple team id goes in one place for the founder to fill in.

Check: read the iPhone project's build settings. **Fixed**. Mobile · affects: Founder

25

LOW

The live site accepted any localhost address to return to after paying

WHAT HAPPENS

After paying, Stripe sends the owner back to an address the server accepts. Besides the portal it accepted any localhost address on any port, on the live site too, not only on the emulators.

HOW TO REPRODUCE

1. Ask the live site for a payment page that returns to a localhost address.
2. Pay and see where Stripe sends you back.

The return address after paying, on the live site

AS RECEIVED

Any localhost address on any port accepted

AFTER THE FIX

Only the portal's address; localhost only on the emulators

THE FIX

Localhost return addresses are accepted only on the emulators.

Check: read which return addresses the server accepts outside the emulators. **Fixed.** Money · affects: Studio owners

Brought or shown by the fixes

Fixes change code, and each round was checked again for what it broke. These came up in those checks and are not among the 25. Most of the second round's came with the in-app purchases added in that round; the ones marked open came up after the third and last round.

HIGH	When a studio paid in the app was handed over, the previous owner's store subscription went on charging them without a word, and the new owner was shown it as their own.	Fixed in round 3
HIGH	A plan given free of charge to a studio paying in the app: the store kept charging while the owner read "Nothing is charged", and the founder's admin didn't show that the studio pays through a store.	Fixed in round 3
HIGH	Purchases made by Apple's reviewers, TestFlight and Google's testers were ignored by the live portal: a reviewer would buy a plan and not get it, a reason to reject the app.	Fixed in round 3
HIGH	No links to a privacy policy or terms in the app or next to the subscriptions, which Apple requires for subscriptions.	Fixed in round 3
HIGH	Found after the last round: moving up with a card for which the bank asks the holder to confirm the payment is reported as "declined", and the server then takes it for the month's last failed payment, ends the paid Studio subscription and moves the studio to Free.	Open
HIGH	Found after the last round, read from the code: a store build set up as the notes say may open email sign-in links in the browser again, and pointing the emails at the website would break email confirmation and password reset in the app.	Open
MEDIUM	After a handover the new owner could move up to Agency at once and pay nothing until the previous owner's paid Studio month ran out.	Fixed in round 2
MEDIUM	Lifting a suspension put the studio back on its paid plan for a month nobody had paid for, and nobody was asked to pay.	Fixed in round 2
MEDIUM	After a move up, the refund of unused time was worked out from the top-up alone, and a full refund of the main payment left the plan running.	Fixed in round 2
MEDIUM	A refund of unused time could be paid a second time if cancelling failed and was retried more than a day later.	Fixed in round 2
MEDIUM	A studio that did pay could be told "isn't paid for yet" and then moved to Free when its billing record didn't say who pays.	Fixed in round 2
MEDIUM	In the store build, the owner of a suspended studio got "Payment details and invoices", which opens Stripe's card page outside the app.	Fixed in round 2
MEDIUM	The sign-in code from the email link reached the app through an address that any other app on the phone can claim too.	Fixed in round 3
MEDIUM	Moving up with a card that declines: Agency started at once without the difference paid, then the studio dropped to Free days before its paid Studio month ended.	Fixed in round 3

MEDIUM	If the store service was slow or down, paying and cancelling on the website failed or hung.	Fixed in round 3
MEDIUM	A member who knows the studio could buy a plan for it from the app outside the normal buttons, and the studio took it.	Fixed in round 3
MEDIUM	A store purchase that had run out kept the paid plan until the store's message arrived.	Fixed in round 3
MEDIUM	If a store's message is lost, a plan can stay paid after the store has given up retrying, or one payment can pay for two studios after a purchase moves between them.	Partly fixed
MEDIUM	A studio paid in one store by another store account can still be offered a purchase in the other store's app (read from the code).	Partly fixed
MEDIUM	One free trial per person: on the live portal an owner whose trial ended by choosing a plan, or whose studio is older than trials, would get a second one. After the last round the second trial is back for "+2" addresses, older records under another +tag and some older member records.	Partly fixed
MEDIUM	Found after the last round: an owner who cancelled and then tries to move up with a card that declines has the cancellation silently taken back; the plan renews and is charged.	Open
MEDIUM	Found after the last round: giving a plan free of charge while the last renewal is failing refunds money from a month already used (this was fixed in the round before).	Open
MEDIUM	Found after the last round: after a handover the previous owner, now a member, can still buy a plan for the studio in the app, and the studio takes it.	Open
MEDIUM	Found after the last round, read from the code: in the US build a plan paid on the website can be changed inside the app and charged straight to the card; a store message can be marked as handled while the store service doesn't answer, so a first purchase waits until the app asks again; for older studios the guess at who pays can pick the wrong person.	Open
LOW	Seven smaller ones from the first round's checks, fixed: the new owner saw the previous owner's payments; a payment already failing before a suspension was still retried; the history said "the plan ended" after any full refund; a handover near the end of a month gave hours of notice; the store build said "isn't paid for yet"; on a phone without the app the link page's main button did nothing; the trial record kept a deleted account's email.	Fixed in round 2
LOW	Ten smaller ones from the second round's checks, fixed: a store's own trial dropped the studio to Free; the founder's change of plan for a studio paid in the app was silently undone; "See plans" led nowhere in the store build; deleting an account paid through a store didn't show where to cancel; a move down in the store wasn't shown; a suspended studio paying in the app was still charged without a word; a failed check after a purchase was never retried; revenue subtracted dispute inquiries; anyone who knew a studio could look up its store purchase; two copies of the portal tidied up each other's subscriptions.	Fixed in round 3
LOW	Smaller ones still open: someone who received a studio during its trial gets no trial for their own first studio; the founder doesn't see an older studio's previous payments after a handover; a payment in the same second as a plan's end can drop a paying studio to Free until the next check; revenue reads every payment on the shared Stripe account when it recalculates; and a few more read from the code.	Open

Checked and fine

- Buying, renewing, a trial without a card, a failed payment that Stripe retries and then gives up on, cancelling to the end of the month, moving up with the difference charged and a partial refund all did what the founder's table says.
- Only the owner can buy, change or cancel a plan: every payment action by a member, a freelancer or the client's people was refused, and only the owner and the founder can read the studio's billing.
- Stripe objects of the founder's other businesses, repeated messages and messages arriving out of order changed nothing.
- When a trial, a payment or a plan ends, nothing is deleted: the usual over-limit rules apply.

- Deleting a studio stops its subscription, and an owner can delete their studio and account inside the app.
- Clients, freelancers and the client's people never see prices in the apps.
- No secret keys in any app build; unencrypted connections allowed only in the emulator build; the release build can't be debugged and asks only for internet access.

Left to the founder

- Stripe's own emails for receipts, refunds and failed payments (finding 18): the switches are named; they apply to the whole Stripe account shared with other businesses, and a separate Stripe account for Folioport avoids that.
- Before publishing the apps: Apple and Google developer accounts, the two plans as store products in RevenueCat with its keys, the Apple team id and signing details for the website links that open the apps, and a Mac or a cloud build for the iPhone app.
- Before taking real money: the live Stripe key and webhook, VAT at Stripe, and the real text of the privacy policy and terms.
- Two rules for the founder to settle: what happens to a plan after a partial refund, and which plan stays when a studio has paid both on the website and in the app (now the store purchase stays and the website subscription is refunded, as asked in the second round).

How it was checked

- The founder's money table written down first: for every event, from buying to a refund, a handover, a suspension or a plan free of charge, what should happen to the plan and to the money; the founder decided the unclear cases.
- Payments on the website run against Stripe in test mode, with Stripe's test clocks moving time through trials, renewals, retries and the ends of periods, and every result compared with the table cell by cell.
- The apps run on an Android emulator, and each build compared with the App Store and Google Play rules on payments, sign-in, privacy and account deletion.
- Fixes sent to the builder in plain words; every round of fixes checked again for what it fixed and what it broke.

Limits

- iOS was checked from the project files and the store rules only: there was no Mac and no cloud build, so nothing ran on an iPhone.
- In-app purchases were tried with RevenueCat's Test Store, not with Apple's or Google's own sandboxes; failed renewals, refunds and a store giving up were checked only through how the portal handles the store's reports.
- The live portal was not touched: everything ran on local copies, with Stripe in test mode, which sends no emails.
- A failure at an exact moment, such as Stripe failing halfway through a message, was made to happen on purpose, or read from the code where it couldn't be.
- Fixes change code: the problems the fixes brought are listed separately and are not among the 25.
- Statuses are after the third and last round of fixes. After it, the handling of repeated and out-of-order Stripe messages was rechecked only in part (it had passed in the round before), and on the phone the sign-in links, files, camera and the screen without a connection were not checked again.

- The Base44 part of the case is reported separately.

Sample engagement: the portal and its studios are fictional and hold test data; it was built with Claude Code for this case; the findings and fixes come from real checks of the build, with Stripe in test mode.