NEWS ALERT
MoviePass accused of misusing customer data after its relaunch

MoviePass: a crisis response plan

Yaaqov Lamb · head of communications, for this exercise

Weeks after MoviePass relaunches, the communications team is celebrating good early numbers. Then that alert lands. I have to decide what happens in the next hour, the next day and the next three months.

A data accusation is bad news for any company. For MoviePass, it's the plot of a sequel everyone has already seen. Where my Adidas case study looks back at a crisis, this one is a plan written before it happens, built on the same idea: values first, proof last.

Why I picked MoviePass

I used MoviePass a lot when I lived in the US. It was amazing, until it wasn't. For a short time it was a real cultural phenomenon, and then it collapsed. That's why the relaunch interested me: the people MoviePass most needs to win back are people like me, who remember both parts.

Previously on MoviePass

The accusation is believable because it fits a pattern people remember.

2018

The then CEO told a conference audience that the app tracked how users traveled to and from the cinema. The company later called this a mischaracterization and apologized.

2019

A security researcher found an unprotected MoviePass database of more than 161 million records, about 58,000 of them with card data. He emailed the CEO and got no reply; the server came down only after TechCrunch contacted the company.

2021–23

Co-founder Stacy Spikes bought the brand out of bankruptcy and relaunched it. Members now earn credits by watching ads on their phones, which points to more data collection, not less.

So the press will not treat this as a one-off. They will treat it as a sequel. The response has to prove this is a different company.

Day one

Hour 0	**Convene the crisis team** CEO, legal, head of security, communications and customer support. First question: what exactly is alleged, by whom, and on what evidence?
Hour 1	**Confirm the facts** Security lists what data we collect, where it is stored and who it is shared with, especially ad partners. Anything in question is paused until it has been reviewed.
Hour 2	**Holding statement goes out** On the website, the app and social channels. Deny nothing we have not checked.
Hour 4	**Brief the people who will be asked** Cinema partners and investors hear it from us first. Regulators hear through legal counsel. Support gets a script and an FAQ.
Hour 8	**Speak to members directly** A plain-language email to every subscriber, a public FAQ for 2019 members who expect “here we go again,” an independent audit announced, and the CEO available to the reporter who broke the story.
Hour 24	Update promised in the holding statement.

The rule I take from 2019: **answer whoever raises the alarm within hours, not after the press calls.**

Who hears it, and in what order

The day-one plan is really a plan about who finds out from whom. For each group, I ask what they will be asking themselves when they see the headline, and who should reach them before the headline does.

1

INSIDE THE BUILDING

Hours 0 to 4

Employees and customer support *"What do I say if a member asks me?"*
A short internal note and a script, sent before the holding statement goes public. Support is the first voice members will actually hear.

2

BEFORE THEY ASK

Hours 4 to 8

Cinema partners *"Will this make our customers distrust us too?"*
A call from the CEO or the partnerships lead, with the facts and the fix, not a link to a statement.

Ad partners *"Is our campaign still running?"*
Told directly, by their account manager, that the data sharing in question is paused. They should never learn it from a screenshot.

Investors and regulators *"Did we hear this from you or from the news?"*
Investors get a call. Regulators hear through legal counsel, so what we say is accurate and on the record.

3

TO THOSE AFFECTED

Hours 8 to 24

Current members *"What do you have on me?"*
A plain-language email and a link to see and download their own data.

Returning 2019 members *"Here we go again."*
A public FAQ that answers the 2019 breach by name, not around it, and the independent audit announced.

The reporter who broke it *"Will they hide or answer?"*
The CEO on the record: what we know, what we do not, and when we will say more.

4

WHENEVER THEY ASK

Ongoing

Wider press and social media *"Is this a pattern?"*
The holding statement, the audit and the 2019 history acknowledged. Silence lets the sequel framing run.

If time forced a choice, I would protect **the returning 2019 members** first. They are few, they remember the researcher nobody answered, and what they conclude decides whether the story is "MoviePass again" or "a different company."

The holding statement

Draft · not for release until every highlighted fact is confirmed

We have seen today's report about how MoviePass uses customer data, and we are taking it seriously. Many of you gave us a second chance, and we know trust is the whole product.

Here is where things stand. [Confirmed fact, e.g. "We do not sell personal data."] We have paused [the data sharing in question] while an independent firm reviews it, and we will publish what it finds. Starting today, you can see and download all the data we hold about you at [link].

We will update you by [time] tomorrow.

[CEO name], MoviePass

Three things to say, three things not to

MoviePass has to earn back trust, transparency and integrity. The members who gave it a second chance are its best witnesses, so every message is written with them in mind.

SAY

1. **Trust is the whole product.** We know what is at stake, and we are not hiding.
2. **Here is what we know, and what we don't know yet.**
3. **You control your data, starting today.**

DON'T

- **Call it a "mischaracterization"** before the facts are checked. That's exactly what happened in 2018.
- **Go quiet,** or put out a statement only a lawyer could love.
- **Joke about it.** The 2022 relaunch event poked fun at the collapse, Hindenburg slide and all. That was a good joke for a comeback. It would be a terrible one now.

Days 30 to 90: earning it back

- **Publish the audit in full,** including anything unflattering.

- **Put a data dashboard in the app,** and make ad-based tracking opt-in only.
- **Name a privacy lead** and introduce them publicly, so there's a real person accountable.
- **Invite returning 2019 members onto an advisory panel.** The people most likely to doubt MoviePass are the ones best placed to keep it honest.

How I would measure it: cancellations against the pre-crisis baseline, sentiment on social media, the share of coverage that mentions the fix and not only the accusation, and support-ticket volume.

What I'm taking from it

1. **The first statement is about values, not facts.** You can say what you stand for before you know everything.
2. **The first person to raise the alarm deserves an answer.** Ignoring the researcher in 2019 is what turned a fixable problem into a headline.
3. **Recovery needs proof people can check.** An audit and a data dashboard do more than any apology.

Sources

- MoviePass app tracks your location before and after movies (MacRumors, 2018)
- Unencrypted MoviePass database exposes sensitive info (MacRumors, reporting TechCrunch, 2019)
- MoviePass pushes forward with comeback (Axios, 2023)
- The return of MoviePass: everything we know (The Week, 2023)