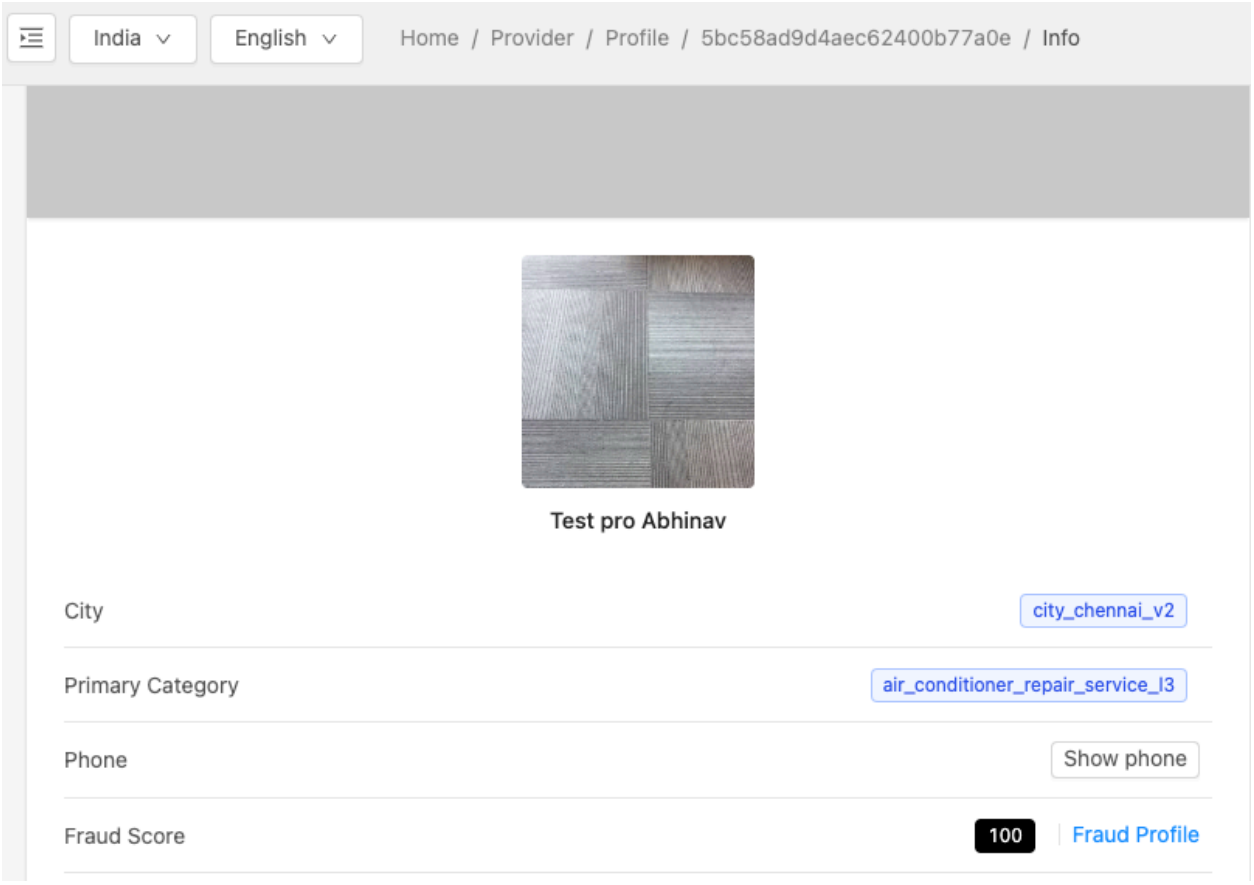
Frauds in UC - overview for business/ops

FIST [Fraud Identification, Safety & Trust] team is the tech team responsible for onboarding, maintaining all kinds of fraud identification, monitoring and actioning, ensuring partner + customer safety and creating greater platform trust, and TnS [Trust and Safety] is the ops team responsible for on-ground implementing/actioning on such matters.

What is a Fraud Score [FS]?

Any entity [partner/customer/agent]'s tendency to commit a fraud can be thought of as a percentage [0-100%] with 5 levels - 0, 25, 50, 75, 100.
Here 0 is the least fraudulent an entity can be, and 100 is the most.
Fraud score increases when an entity commits -

1. More counts of the same fraud, and/or
2. More types of frauds



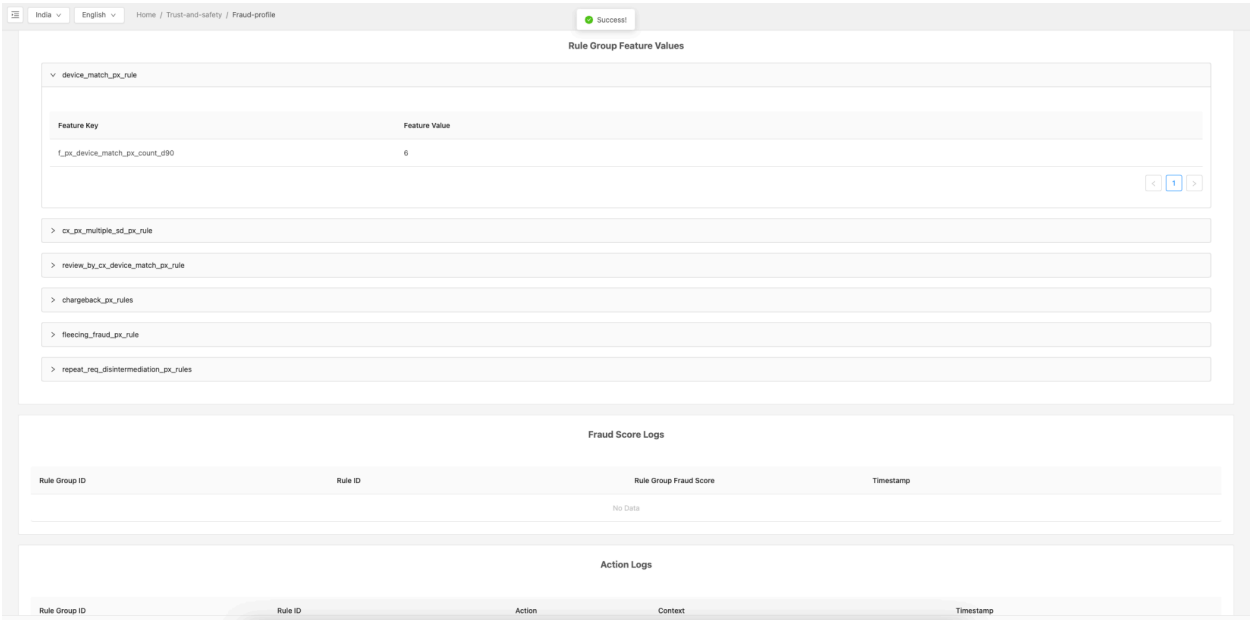
Why do we need FS?

To proactively correct behavior, churn bad actors and ensure a safe marketplace for customers and partners.

How is FS calculated?

FS calculation is complex - multiple types of frauds combine to make the cumulative FS what it is.
The calculation mechanism is confidential and restricted to the FIST tech team and is not divulged to the broader org to prevent data leaks to customers/partners who might find ways to game the logics.

In short - Fraud rules are a complicated calculation based on indicative flags, calculated over a rolling window i.e. we check counts of frauds happening over the last X days and not through the entire partner/customer [AKA entity] history. It's possible an entity was fraudulent in the past, but since we identified them as fraudulent and took preventive measures, their fraudulent behaviour reduced/died down. Hence it becomes important to look at only the most recent fraud history.



What are the frauds which are currently being used?

1. Same Cx-Px pair doing multiple bookings in a short period of time
2. A customer who was blocked is trying to make a new UC account [different number/email] from the same device
3. If partner gets a rating from his own mobile device [i.e. partner is trying to rate himself by making a fake customer account]

4. If partner sends a request and accepts it from the same mobile device [i.e. partner is trying to do bloat up the #leads they do]
5. If customer cancels a lot of leads after responding
6. If customer raises a lot of refunds
7. If partner raises a lot of refunds [or drives a lot of refunds with poor service]
8. If partner tries to overcharge [this is called fleecing] a customer/UC by artificially bloating the bill
9. If customer books a lot of cross gender services [male customer repeatedly booking a female massage/salon therapist]
10. Credit card chargebacks done by the customer [international geography]
11. Disintermediation - partner trying to deliver an off-platform service.

Appendix

For further questions about frauds, trust and safety, reach out to the following POCs -

1. Product - Durjai Sethi
2. Trust and Safety, Risk Management Group Ops - Kamal Yadav / Ayushi Srivastava