Shared data from alliances will prevent airline mileage fraud
Abstract

Airline loyalty fraud has existed for long, but it is only of late that preventing it is getting proper attention. A kind of fraud that was dismissed — ‘It’s just points, not real money’ — has become a digital currency now, and its scale is hitting airlines’ bottom lines. As airlines feel the financial crunch due to the COVID impact, they are exploring all avenues to plug gaps and leaks, and tighten processes to reduce losses, even of digital currencies like loyalty points. The loss due to loyalty fraud is massive when fraudulent activities on all the airlines of an alliance are considered.

How mileage accrues in an alliance

Generally, passengers in a frequent flyer program (FFP) can accrue miles for flying on any operating airline (OPE) that is part of an alliance. The alliance facilitates information exchange between member airlines via intermediate systems (often called ‘hubs’). Today, only the data relevant for mileage accrual is exchanged between alliance members. The accrual process is generally automated—the OPE sends the details of the travelers to the FFP. Members who don’t receive miles via the automated process post flying can log in to the FFP’s website and raise a retroactive mileage claim request, which is sent to the OPE for validation. When these options fail, helpdesks of the airlines concerned help passengers accrue miles.

Loyalty fraud can take various forms

Airlines of an alliance don’t have the complete information about FFP members and their travel. The operating airline usually has only the travel information of the passenger (from their source systems like the departure control system (DCS) or the global distribution system (GDS)) and the FFP generally has only the member-related data. Fraudsters usually exploit this gap in information to cheat airlines. For eg, fraudsters may enroll in an FFP program with a name common for their geography, say ‘John Smith’, and raise retroactive mileage claim requests on long-haul flights on different OPEs. The OPEs only check if a ‘John Smith’ was present on the flight. If there was a John Smith or a Johnathon S (an actual passenger with the same or similar name), the OPE system may deduce that it is the same FFP member and approve the request. The operating airline has only the passenger’s details and travel details. Hence, validations are done based on the combination of these details (Eg: passenger name + flight departure date + origin + destination + flight number). The OPE is not in a position to verify the FFP number.
There are also complexities in matching very long names (the FFP may have some part of the name but the OPE may have the ticketed name stored differently) or very short names (a fraudster using the name ‘Li Li’ may get mapped to ‘Lima Li’ or ‘Anakeli L’). In short, name match validations are tricky for airlines. While a 100% name match is impractical, a very lenient name match algorithm exposes the airline (and, in turn, the alliance) to fraudsters, making detecting and handling them difficult. It is even harder to find internal fraudsters (within the system). Airlines have to spend serious time and effort to determine and block fraud — a major reason why many airlines do not think it worthwhile to dig deeper into such cases.

Fraudsters target OPEs with weaker algorithms, bombarding their systems with a huge number of requests (via scripts and BOTs) using very short passenger names (hoping that it will pass the name match validations of the OPE concerned due to a partial match with an actual passenger’s name). But, when a fraudster targets all the OPEs in an alliance, each OPE individually may not be able to see a fraudulent pattern. Also, since the OPEs compensate the FFP for miles awarded, the FFP does not see an incentive in putting in additional checks as that would make it more difficult for its genuine members to raise requests. This leaves the OPEs to fend for themselves.

There are other modes as well to hoodwink the automated accrual process. There have been cases of third-party or airline agents entering their own FFP number for bookings made with them by flyers not part of any FFP—the agent gets miles without even travelling! There could be rogue characters within the loyalty or backend IT departments tweaking the FFP number before the information is transmitted from the OPE to the FFP (or in between). It is difficult to detect such frauds.

There have also been cases of double dipping (where a person opens an account with multiple FFPs, raises retroactive mileage claims from more than one account to claim miles multiple times for the same travel), stealing or sharing FFP member account passwords, and account takeovers. But airlines have taken steps to prevent such attempts. In programs that allow pooling of miles into a single account (ideally intended for people from the same family), fraudsters collect small amounts of miles/points and then pool them all together into a single account to make a redemption. Besides, fraudsters also claim miles by creating new FFP accounts with stolen PNR information, selling redemption tickets and loyalty information on the dark web.

Why alliances need to act

The FFP has very little incentive to prevent fraud as it is the OPEs who pay an FFP member for miles. The OPEs do not have any means to look at the profiles to ascertain if an FFP request is genuine. There may also be cases where a single OPE may not even be able to detect the fraud (as the fraudster may have targeted multiple OPEs, sending only a few requests to each OPE). The alliance has a broader view of all FFP transactions with all OPEs. This comprehensive data can help provide insights into fraud patterns and help put in measures to combat them.

Moreover, a central solution at the alliance hub will ensure the benefits are realized immediately by all member airlines. The costs as well get shared between the member airlines, leading to maximum benefits with minimal costs (as compared to each airline building its own elaborate systems and checks).
What the FFP loses

It is common belief that the FFP loses nothing when fraudulent miles are claimed. However, there is the redemption aspect to be considered. Generally, most FFPs provide more redemption options on their own airlines. As many FFP and OPE entities (even when they are within the same airline) behave as separate entities, the FFP compensates the OPE monetarily for all redemptions made (the FFP deducts miles/points from FFP member’s account for services provided by the OPE, and financially compensates the OPE). The OPE, on the other hand, ends up providing services to a fraudster (instead of a genuine FFP member) and has to also bear the opportunity cost—it loses ticket revenue on the seat booked by fraudsters by redeeming miles. Given the number of fraudulent miles being claimed and the ease with which they can be redeemed, the FFP stands to lose quite a bit by allowing fraudsters to exist in the FFP program. When the redemptions are made on other partners/airlines (other OPEs), the FFP ends up compensating the partners for the services provided as well.

The OPE pays the FFP for the miles it authorizes to be provided to an FFP member (for the member’s travel). There could also be cases where a genuine passenger requests for miles (for travel) but finds the miles already credited to a fraudster. In such cases, it is generally the FFP that absorbs the cost for mileage accrual as the OPE would have already approved the miles for the flight activity based on the first request.

Airline alliances can prevent such frauds

Airline alliances have a big role in preventing such frauds. To begin with, an alliance should inspect the humongous data it has and look for patterns indicating potential fraud. It can, for instance, check the mileage accrual requests to figure out if there are FFP members who seem to be travelling around the world and back—all in the same day. Retro requests raised in the blink of an eye could alert the alliance to potential fraud as BOTS could be behind such requests. The alliance, at this stage, may not be able to zero in on the fraudster. It could, however, make reports available to member airlines, which can help FFPs and OPEs detect frauds and make their systems stronger to prevent them. Alerts could be put in place to let FFPs know that something seems to be out of place (for eg, over 100 requests from an FFP member in an hour, or many requests with the same ticket number from one or multiple FFP members should raise an alarm).

The next step would be to put in place blocks for cases that seem to be suspicious. These could be based on configurable thresholds (for eg, all retroactive mileage claim requests can be blocked if more than 10 requests have been received from an FFP number already in the same day). The FFPs would then have to review the account activities for all the blocked FFP members and confirm if the members are genuine.

The alliance can also facilitate exchange of key member data (like date of birth, date of enrollment) to the FFP program, to ascertain the genuineness of a claim. The ideal step would be the creation of an automated, machine learning-based model trained on existing data within the alliance, that can be used to predict whether a mileage accrual request is genuine.

In a world where fraudsters are innovative, an airline alliance, along with its members, will have to look for solutions that are unique and futuristic to prevent them.
About the authors

Vipin Venugopalan, business analyst - TCS

Vipin has over 8 years of experience in the airline domain (over 4 years of focussed experience in helping airlines deal with inter-airline loyalty fraud). He works as a business analyst for Star Alliance and specialises in loyalty and baggage handling domains.

Vasantharaja K, delivery owner - TCS

Vasanth has over 17 years of experience in the airline industry and has been involved in providing solutions for multiple airlines and airline alliances. He has been a part of multiple teams to create industry-first inter-airline solutions.
Awards and accolades

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is a purpose-led transformation partner to many of the world’s largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge. TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company’s 500,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit www.tcs.com and follow TCS news @TCS.

Contact

For more information on Travel, Transportation and Hospitality, visit https://www.tcs.com/

Email: marketing.tth@tcs.com@tcs.com

All content/information present here is the exclusive property of Tata Consultancy Services Limited (TCS). The content/information contained here is correct at the time of publishing. No material from here may be copied, modified, reproduced, republished, uploaded, transmitted, posted or distributed in any form without prior written permission from TCS. Unauthorized use of the content/information appearing here may violate copyright, trademark and other applicable laws, and could result in criminal or civil penalties.

Copyright © 2022 Tata Consultancy Services Limited