ibssoftware

ibsplc.com

Fighting fraud in airline loyalty programs

How new technologies help airlines protect loyalty points and members from fraudulent behavior

Loyalty fraud – a global problem for airlines

Across consumer industries, a global increase in online fraudulent behavior is driving awareness of the shortcomings in existing fraud management policies and technologies. Airlines are the most affected by online fraud, accounting for 46% of fraudulent transactions, where airline loyalty fraud is among the most "widespread, increasing and far-reaching," IATA reports.

Airline executives are awakening to this new reality, where airline loyalty fraud alone costs airlines millions of dollars every year. Shockingly, the fraudulent redemption of airline loyalty miles amounts to a $3.1 billion problem worldwide, according to the Loyalty Fraud Prevention Association.

In addition to financial losses, airlines face reputational and regulatory damages due to loyalty fraud. "Fraud cases lead to significant reputational impacts on the impacted institution, with the additional reputational loss predicted to be ~140% of the announced loss," according to Oliver Wyman.

Fortunately, emerging fraud management technologies that integrate with airline loyalty programs are improving how airlines recognize loyalty fraud and then act to protect their loyalty programs, brands, and customers.

The state of airline loyalty fraud today

> *"Methods that fraudsters use are varied and innovative. Social engineering, machine learning, and artificial intelligence are just a few examples. It is a constant game of one-upmanship going on between the fraudsters and those trying to prevent fraud."*
>
> **— IATA, "Fraud prevention: Strengthening the defenses."**

Airlines, loyalty members, and fraudsters alike have recognized the equivalent cash value of loyalty points for years. But the onset of the global COVID-19 pandemic solidified this connection as airlines were forced to cancel flights. Subsequently, both members and fraudsters looked to use loyalty points not necessarily for air travel but for alternative gains—both legitimate and illegitimate.

A growing black market

Loyalty points, regarded as "soft money," were less targeted when loyalty programs were simple. But stealing and trading loyalty points has become a lucrative business among criminals on the dark web.

From Security Intelligence: "Today's [legitimate] loyalty program industry is a large ecosystem of partners offering purchases through Frequent Flyer points," acknowledges Chris Staab, co-founder of the Loyalty Fraud Prevention Association (LFPA). "On the dark side, you have 'mileage brokers' that illicitly buy and sell points to exploit them."

Airlines must take meaningful action

Fraud detection and prevention can no longer be an afterthought for airlines, many of which struggle to identify who is using their members' loyalty points and how they are using them. Airline executives must begin by understanding the major types of loyalty fraud and how they've become so problematic to date.

The three most common types of loyalty fraud

As stolen airline loyalty points grow in demand, fraudsters are developing new ways to exploit member data and loyalty points. There are three primary types of loyalty fraud airlines face today, each with unique personas and methods.

1 Internal fraud

Internal fraud is perpetrated by current or former airline employees, site staff, administrators, and agents, among other industry "insiders." 10% of fraud or misuse of loyalty accounts is committed by airline staff, according to IATA. This fraud is difficult to detect and prevent because the fraudsters have legitimate access to member data and account information.

2 External fraud

External fraud is committed by people outside the industry, such as criminal organizations. These criminals steal loyalty points through various methods like data breaches, phishing attacks, member account takeovers, identity theft, and social engineering. According to IATA, "loyalty account theft" is the second most common type of airline loyalty fraud.

3 Gaming fraud

Gaming fraud, also called "friendly fraud", is perpetrated by members who game an airline's loyalty system to earn points to which they are not entitled. Gaming fraudsters often exploit airline rules and loopholes to accelerate their earnings or redeem points for more value than they should. In one famous example, a loyalty member bought 12,000 pudding cups as part of a promotion to acquire $25,000 in loyalty points.

Loyalty fraud translates to real losses for airlines

Though loyalty points "belong to members," they are not independent of airlines' financial assets. "Loyalty programs generate revenue, as well as being important sources of customer data," says IATA. "It is therefore in the interests of airlines to protect this investment in customer relations".

Facing reputational damage

Airlines face additional losses from reputational damage due to loyalty fraud. The reputational damage of large-scale fraud can be considerably more than the immediate value lost in the attack itself.

Prioritizing AI- and ML-driven technologies

As airline CFOs are increasingly held accountable for loyalty fraud losses, they are looking to adopt new fraud management technologies. And these solutions must be able to detect and prevent fraud in real-time using machine learning-based fraud detection models that are constantly updated with the latest intelligence to be effective.

Progress towards combating airline loyalty fraud is slow

Compared to industries like banking and retail, air travel is behind in terms of fraud management technologies and capabilities. Most existing fraud management solutions for airlines use legacy rules-based systems that cannot keep pace with fraudsters' rapidly evolving methods. Some airlines continue to rely on slow manual processes for detecting and responding to fraud as well.

Fraud and loyalty departments fail to connect

Too often, these departments operate as different business entities within an airline. Software that automatically detects fraud in defined documents, historical data, and other unique elements of loyalty departments and their programs can help bridge the gap between these two teams. Unsupervised fraud detection models use AI and fraud modeling without human involvement, freeing both parties from manual labor as well.

Emerging loyalty management technologies for airlines

Fortunately, airlines have access to a broad range of fraud prevention, detection, and management technologies that bring new intelligence to loyalty programs. Moreover, these technologies can integrate with their existing, or entirely new, loyalty programs and systems.

These technologies have two capabilities that set them apart:

I. Automatic Detection

Intelligent loyalty fraud technologies include a detection mechanism for defined, suspicious behavior. These technologies employ pattern recognition to identify fraudsters' methods as they happen and prevent loyalty points from being transferred or redeemed. AI assigns a risk score to certain accounts, with different layers of approval required when questionable activities occur, for example:

- **Activity from blacklisted IP addresses**
- **Inactive accounts suddenly activated**
- **Suspicious buying between accounts**

How is this better?

These new solutions are powered by machine learning, featuring statistical regressions that enable them to detect fraud automatically without static rules or human intervention.

II. Self-Learning

In addition to automatic detection, intelligent fraud management technologies for airlines have self-learning capabilities that monitor data in real-time to uncover new fraud patterns. Machine learning fraud models are constantly updated with the latest fraud intelligence, so they can adapt as fraudsters' methods change.

How is this better?

Existing tools require fraud teams to manually update rules-based systems, which is time-consuming and error-prone. The sheer volume of data means manual processes are inefficient or nearly impossible. Self-learning means airlines can proactively combat fraud rather than react after the fact. Airlines needn't make heavy investments in additional staff or training, either.

Critically, both technologies integrate with new or existing loyalty software to improve visibility, adaptation, and outcomes, as well as reduce manual tasks and interventions.

Countermeasures for all types of loyalty fraud

With these new tools, airlines have targeted capabilities for combating fraud in all categories: internal, external, and gaming fraud. Here are the countermeasures to mitigate several types of fraud:

Internal fraud

- Automated monitoring and alerts for all critical program KPIs
- Monitor overall and partner liability
- Detect unusual activities in an automated way
- Tamper proof audit records

External fraud: Account takeovers

- Enable real-time behavior analytics
- Classify unusual activities into suspicious and unsuspicious actions
- Automatically detect suspicious login activities
- Detect fraudulent redemptions or transfer transactions

External fraud: Fake Accounts

- Define the maximum limit of referrals per member per month
- Use smart data validation (e.g., via email, mobile, address)
- Detect suspicious traffic from bots
- Automatically detect patterns and flag or suspend membership accounts

Gaming fraud

- Set smart thresholds in the Terms & Conditions and the loyalty platform
- Define maximum redemption, conversions, and transfers from other programs
- Enable real-time behavior analytics

Loyalty fraud will only get worse

While the value loyalty programs add to airlines and members is clear, protecting these assets often comes as an afterthought. But as cybercrime becomes increasingly sophisticated and ingenuous, airline reputation and financial risk will only grow over time. Airlines will need to be more proactive about fraud prevention and detection to keep up with increasingly disguised threats to their loyalty programs and members.

Fortunately, AI and ML-based models are game-changers for fraud prevention, detection, and protection. These technologies can perform deeper and faster behavioral analysis on transaction patterns to stop fraud at the door, alleviating airline teams from complex manual processes and financial write-offs. Only by combining increased management attention to fraud with the latest purpose-designed technologies will airlines be able to safeguard their loyalty business and program members.

iloyal

Leading airlines worldwide use IBS Software's iLoyal platform to power their reward schemes and drive member engagement with their loyalty programs.

Underpinned by a highly configurable SaaS platform, the solution gives airlines the freedom to innovate and quickly deploy new products and services. Thanks to its open and cloud-native design, iLoyal facilitates partner integration, accelerating value delivery to airline loyalty program members.

The platform provides airlines with a 360-degree customer view to personalize relevant offers to their members through sophisticated data and analytics capabilities. Real-time transactions enabled, from search to redemption to fraud prevention, iLoyal's secure platform drives program growth and revenues for the world's top airlines.

About iLoyal and fraud prevention

Using advanced data analytics and ML models, iLoyal's fraud prevention and detection solution monitors transactions in real-time to keep airlines and their members safe from illicit activities. The solution integrates seamlessly with your existing IT infrastructure so you can begin fighting fraud immediately. Get more details on how to create a fraud-free loyalty program →

ibssoftware

Contact us

Engage, grow, and adapt with IBS Software.