The Dark Side of Loyalty: Combating $1 Billion Frequent Flyer Mile Scams in the Airline Industry

Frequent flyer programs have long been a symbol of loyalty and reward in the airline industry. These programs are intended to reward travelers with benefits and encourage ongoing customer relationships. However, a growing and pervasive threat is lurking beneath the allure of free miles and exclusive perks: Frequent Flyer Miles fraud. **At the last credible count in 2018, there were over 30 trillion unspent miles in circulation**, according to McKinsey.

It's no surprise that cybercriminals have zeroed in on these loyalty programs as lucrative targets, presenting a massive financial risk for airlines. As fraud continues to rise, airlines must reassess their approach to protect the value and integrity of their loyalty systems.

What is Frequent Flyer Miles Fraud?

Frequent Flyer Miles Fraud involves cybercriminals accessing airline loyalty accounts to steal points or miles with real-world value. They achieve this through methods like credential breaches, phishing, or exploiting weak security. Once inside, fraudsters swiftly redeem or transfer the stolen miles, often selling them on underground markets for profit.

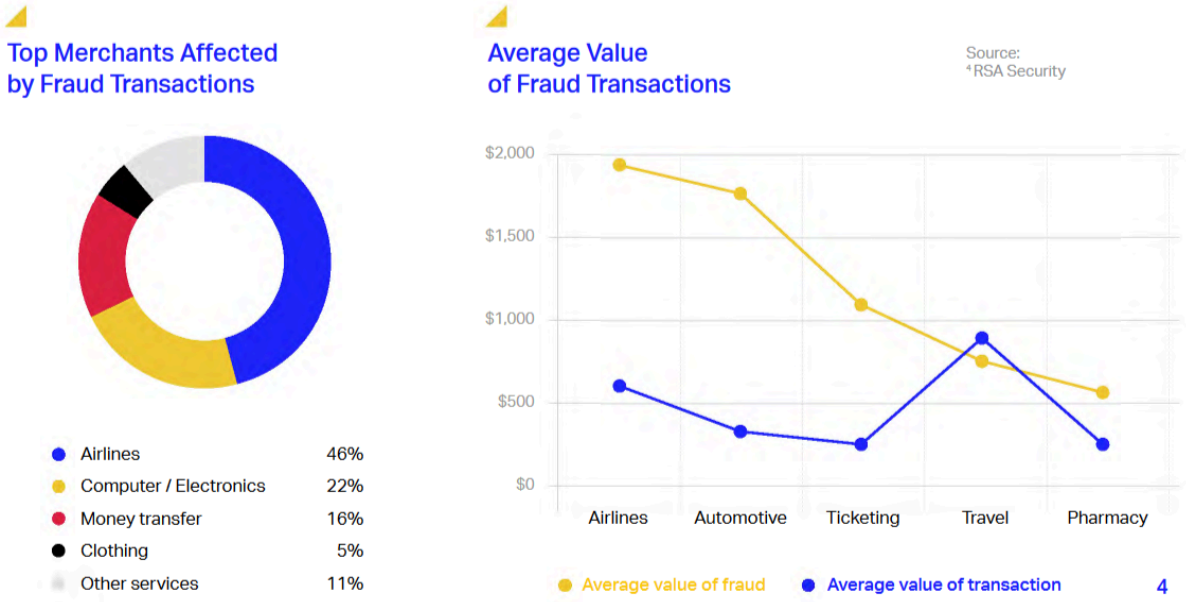
Types of Frequent Flyer Miles Fraud:

- **Account Takeovers**: Hacking into legitimate accounts to steal points. This is often achieved via impersonation scams leveraging the usual phishing-related techniques and fake websites used to lure unsuspecting airline customers into handing over credentials.
- **Fake Accounts**: Creating counterfeit accounts to illegitimately accumulate rewards.
- **Insider Exploitation**: Employees abusing their access to loyalty data for personal benefit.

Source: International Air Transport Association (IATA)

What Makes Frequent Flyer Miles Fraud Such a Pressing Concern for Airlines?

According to the International Air Transport Association (IATA), frequent flyer fraud contributed significantly to making **the travel industry responsible for 46% of all fraudulent transactions in 2023**, costing airlines over $1 billion.



Source: RSA Security

Airlines often focus on payment fraud, measuring it by chargebacks and rejected bookings. **In North America, rejected bookings are nearly double the 3.8% global average**, suggesting a larger loss of valid orders. This highlights a major vulnerability in the industry's defenses, potentially increasing customer frustration due to difficulties in redeeming rewards.

Customer Trust and Loyalty: Fraud significantly undermines customer trust. When frequent flyer miles are stolen, affected customers lose confidence in the airline's ability to protect their accounts, damaging the brand's reputation and negatively impacting long-term loyalty. Customers who feel unprotected are less likely to remain loyal or continue using the airline's services.

Financial Loss Beyond Fraud: The financial impact of frequent flyer fraud extends beyond the direct theft of miles. Airlines face increased costs in fraud prevention measures, customer support to address fraud incidents, and potential legal fees. These operational costs add up, making fraud a significant drain on resources.

Operational Disruption: Fraud also leads to operational disruptions, as airlines need to handle increased support requests, customer disputes, and manually review fraudulent activities. These disruptions divert valuable resources away from core operations and can affect overall service quality, further eroding customer satisfaction.

Frequent flyer miles fraud, therefore, is more than just a financial hit—it's a multi-faceted issue that affects brand loyalty, operational efficiency, and overall customer satisfaction.

https://youtu.be/PHuWZ1opDpk?feature=shared

Why Incumbent Solutions Fall Short

Traditional approaches to combating Frequent Flyer Miles fraud have primarily relied on rule-based mechanisms and post-event fraud detection, which often result in delayed identification and mitigation of fraudulent activity. This outdated approach leads to increased operational costs, higher chargebacks, and potential reputational damage.

Incumbent solutions often lack proactive capabilities, relying instead on reactive responses that only address fraud after it has already occurred:

- **Lack of Proactive Threat Detection**: Traditional systems wait for fraud events to occur before taking action, leading to delayed mitigation and increased impact.
- **Delayed Monitoring**: Without real-time browser-based monitoring, many systems are unable to detect early common techniques for breaking into loyalty accounts, like credential stuffing attacks.
- **High False Positives**: Incumbent solutions struggle to distinguish between legitimate and fraudulent behavior effectively, leading to increased false positives and negative customer experiences. This results in operational inefficiencies and customer dissatisfaction.

Memcyco's Capabilities to Pre-emptively Roadblocking Frequent Flyer Miles Fraud

Memcyco addresses the key shortfalls of traditional, incumbent solutions with its advanced capabilities, categorized into 'Detect', 'Protect', and 'Disrupt' pillars:

- **Detect the early signs pre-emptively**: Memcyco excels at detecting pre-scam anomalies and tracking attacks from the onset. With real-time monitoring, Memcyco detects suspicious behavior, including credential stuffing attempts, early-stage attack indicators, and device anomalies. This capability ensures that airlines are always a step ahead, able to identify threats as they develop.
- **Protect loyalty account credentials**: Memcyco's protective measures include locking out attackers while ensuring genuine users can still access their accounts. Features like Device DNA help airlines trust known user devices implicitly without adding friction, thus maintaining the customer experience while blocking unauthorized access. Moreover,

Memcyo's device DNA can actually help identify every user who clicked on a phishing to an impersonating site, or imputed their credentials.

- **Disrupt**: Memcyco doesn't just play defense—it also disrupts scams in progress. This includes u**sing decoy data to mislead fraudsters**, automated takedown of impersonation sites, and SEO poisoning to lower the visibility of fraudulent websites. By actively disrupting the mechanisms of scams, Memcyco limits the ability of fraudsters to succeed, helping to protect both airlines and their customers.

- **Proactive Threat Detection**: Memcyco overcomes the reactive nature of traditional systems by **using predictive modeling to flag suspicious activity before it turns into fraud**. This proactive approach enables early, upstream intervention, reducing the overall impact of fraud incidents.

- **Real-Time Browser-Based Monitoring**: Unlike delayed detection methods, Memcyco's monitoring takes place at the browser level in real time. **This allows for immediate identification and blocking of unauthorized access attempts**, including early-stage attacks like credential stuffing.

- **Enhanced User Experience**: Memcyco significantly reduces false positives compared to traditional solutions. By distinguishing legitimate user behavior from fraudulent activity more effectively, Memcyco minimizes disruptions for genuine customers, leading to a smoother and more satisfying user experience.

Secure Your Frequent Flyer Loyalty Revenue, with Memcyco

Frequent Flyer Miles fraud is more than just a nuisance—it directly impacts your bottom line. It's time to proactively strengthen your defenses, protect valuable loyalty program revenue, and ensure your customers feel secure and valued. With Memcyco's 'Detect,' 'Protect,' and 'Disrupt' capabilities, you can turn the tide against fraudsters, protect your earnings, and maintain customer trust. Ready to level up your defenses? Let's work together to keep your loyalty program—and its revenue—safe.

Book a Memcyco demo and discover the real-time AI-assisted capabilities helping airlines save millions in loyalty program airmiles theft.