ARKOSE LABS | LSA LOYALTY SECURITY ALLIANCE

The Silent Threat: Unmasking Loyalty Fraud & Account Takeover in the Digital Age

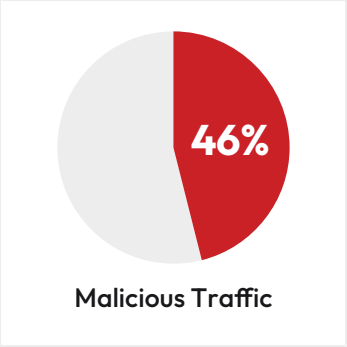
Part 1: Survey of the consumer experience

Key Findings:

- Up to **5%** of Loyalty Program Members have had their accounts compromised.
- Value stolen from these accounts estimated to be **$1,000 to $5,000** for those that had points transferred out.
- Loyalty programs are leveraging cyber and other tools to enhance member protection, with **50%** of respondents reporting account compromise but no value taken.

The past few months have seen a plethora of major global brands fall prey to large-scale data breaches. Most recently, Qantas, Australia's flag carrier, had 5.5 million customer records stolen – a figure equivalent to the entire population of Scotland! At the time of this writing, the full impact in terms of Account Takeover (ATO) or compromises for Qantas' Frequent Flyer Program customers remains unknown.

Australian consumers are deeply engaged with their loyalty programs, and comprehensive consumer research reports on their attitudes are published annually. In the 2018 "For Love or Money" report and this year's version, respondents were asked if they had been victims of an account takeover. This year, 8% of respondents confirmed they had, a significant increase from the 3% reported in the earlier survey. These numbers corroborate what companies like Arkose Labs are observing across their client networks



Malicious Traffic

A recent Arkose Labs report on threat actor behavior found that fraudsters targeting airlines upped their game late in 2024. In Q4, advanced bots represented more than **46%** of malicious traffic, suggesting that scammers see unique opportunities in the airline industry that warrant customized, highly targeted strategies rather than commoditized attack toolkits.

What those broader surveys often don't reveal is the specific value taken from compromised accounts, nor how the account holder discovered the fraud. Furthermore, once an account was compromised, how effectively did the program manage the situation and support the victim? Account security firm Arkose Labs and the Loyalty Security Alliance (LSA) set out, through a targeted straw poll, to answer some of these critical questions.

The LSA was established to help the loyalty industry better protect its programs from fraud. As part of Airline Information, we contacted a random sample of our collective database, asking a small number of questions about their experiences with Account Takeover and compromised accounts. Arkose Labs works with the world's largest B2C companies, including airlines, banks, retailers, etc. to help secure loyalty programs from ATO, ghost account creation, inventory hoarding and other types of attacks.

We received 133 responses, and 30% of these confirmed that they have fallen victim to fraud. Our combined LSA

and Airline Information database is naturally skewed towards individuals in the travel sector. This bias is reflected in the types of accounts our respondents reported as compromised. What's clear from our data is that some respondents had more than one account compromised. One of the persistent challenges in protecting accounts is the widespread use of recycled passwords. Fraudsters are increasingly leveraging AI at scale to conduct brute-force attacks, enabling them to compromise multiple accounts far beyond the initial data breach.

10k

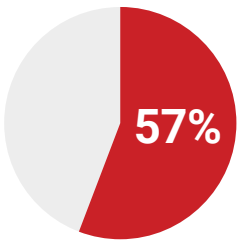
Malicious Bookings

Travel booking sites are facing persistent threats from cybercriminals. The scammers are using bots to commit credential stuffing at scale to compromise user accounts and steal accrued loyalty points. Plus, fraudsters are launching inventory hoarding schemes that can shatter user trust. Prior to working with Arkose Labs, a major APAC-based airline affected by this type of attack was experiencing **10k** malicious booking attempts monthly, leading to the airline losing up to 30% of its traffic.

Travel is frequently perceived by fraudsters as offering the greatest potential value within compromised accounts. This is partly driven by the immense scale of these programs – for instance, Delta Airlines alone has billions of US dollars in liabilities on its balance sheet for rewards. Moreover, these rewards can often be easily converted into cash or near-cash equivalents, not just a hotel room or a flight.

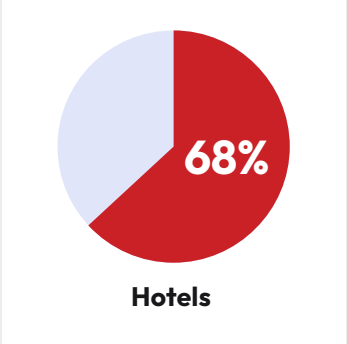
It's interesting to note the comparatively lower number of Banking/Financial Reward accounts reported as compromised in our survey. This raises a pertinent question: Is this because fraud prevention measures are inherently stronger at banks, or do fraudsters simply perceive them as harder targets, preferring to exploit loyalty programs?

Most programs are diligently working to prevent unauthorized access to both their corporate systems and the loyalty program accounts within them. We know from discussions with various programs – including Qantas – that corporate systems are under constant attack.



Airlines

According to an Arkose Labs study, 57% of airlines report that AI-powered solutions are giving them enhanced defenses against human fraud farm attacks—an area of concern particularly in industries with high levels of customer loyalty programs, which are often prime targets for fraudsters.



Hotel loyalty programs are at risk, too. **68%** of hotels are concerned about loyalty point theft and fraud. Often used along with account takeover attacks, seizing control of a customer's unused loyalty points increases the value of attacks for fraudsters. This practice stands to frustrate good users and devalue the loyalty program for legitimate customers.

Top-tier programs, equipped with state-of-the-art cybersecurity, can detect breaches of their prevention processes almost instantaneously. At that point, the focus shifts to cyber-level detection. However, attacks that occur at a more "granular" level, targeting individual accounts, can often be harder to spot, leading to successful account takeovers or compromises.

So, while cyber teams might be aware of corporate system compromises, how did our survey respondents discover the attempt at fraud on their loyalty accounts? Interestingly, it appears programs are becoming more proactive, as almost half of respondents (48.6%) stated they were "locked out of the account" when trying to log in. Programs typically implement these lockouts the moment an anomaly is detected.

Other methods loyalty programs are using to alert their members include emails about suspicious account activity, which alerted almost 1 in 5 respondents. Additionally, 28.6% of eagle-eyed members spotted suspicious activity themselves. While programs have increasingly adopted Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA), surprisingly, only 11.4% of members realized something was wrong through an uninitiated 2FA/MFA request.

The challenge of recycled passwords, as mentioned previously, is a persistent vulnerability for any online account. Our results further underscore this: almost 1 in 5 respondents had experienced a compromise on another loyalty program account and subsequently checked their other accounts. This clearly demonstrates that fraudsters are operating at scale, often leveraging AI, to crawl the web, attempting to access multiple accounts with stolen credentials – and often succeeding.

> "Overall terrible experience with Ulta loyalty program. Now I no longer save up my rewards to spend at Christmas; I use them as soon as I earn them."
>
> — Loyalty Program Consumer

What Are Fraudsters Doing Once Inside an Account?

The Dark Web is unfortunately replete with loyalty accounts for sale, often explicitly stating the value held within them. Unsurprisingly, the highest-value accounts are those that have been completely drained. Just 1 in 20 of our respondents (5.3%) were unlucky enough to fall victim to this total clearance. For those who experienced point theft, the reported values

ranged from $1,000 to $5,000 USD.

Encouragingly, at least half of our respondents (50%) had nothing taken from their compromised accounts, indicating that program systems are indeed improving significantly at protecting accounts once a compromise is detected. However, the other 50% did have value stolen, ranging from partial to full depletion. If these numbers are replicated across the industry, the cumulative sum that programs are forced to replace is considerable.

Indeed, one of the newest and most insidious ATO fraud schemes involves two loyalty programs. The initial compromise occurs in Program A, and the points are then transferred to Program B. When these points arrive in Program B, the transfer appears legitimate, as Program B's account itself hasn't been compromised. The redemption then takes place from Program B, appearing entirely normal until the account holder at Program A eventually realizes what has happened. Program A is then not only obligated to restore their member's previous balance (a significant cost) but may also face additional costs related to the points that were transferred to Program B. This effectively doubles their financial exposure.

The survey responses also shed light on how programs handle these compromises. First-party fraud (where the member might be complicit or abusing rules) and "program abuse" (e.g., non-compliance with terms) can occur. Our data shows that in approximately 1 in 5 cases, the program closed the member's account, and a further 9.1% reported their account was still suspended. This highlights the difficult decisions programs face in managing suspected abuse.

However, despite the challenges, there's a positive note: even though 45.5% reported difficulties in getting value restored, 4 out of 10 (40.9%) did get put back to their pre-fraud position. Naturally, managing a loyalty program at scale, with 5-8% of accounts potentially compromised (based on LSA and "For Love or Money" research), is incredibly time-consuming. This makes the emphasis on prevention – at both the cyber team level and the program design level – all the more critical.

Comments from Loyalty Program Consumers and Survey Respondents

"The entire experience felt like it was to protect the airline and any inconvenience to me was not even recognized. Including things like giving up an account number, calculating million miler status, non-points awards, and stored information."

"This was a program which was run by an airline. The airline ceased to operate and before closure it spun off the Loyalty management into a separate company. Even that company is closed."

"Two factor authentication has been the factor in this not repeating."

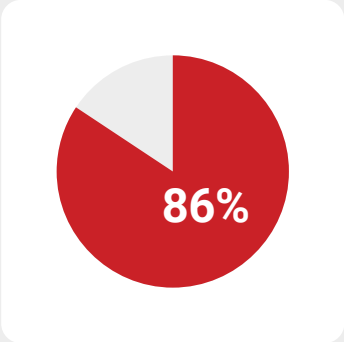
"Zero contact from the program. Zero effort to fix the issue."

"I was the victim of a large hotel breach that took a lot of PII and fraudsters were able to open a PayPal line of credit in my name with the stolen data."

"Attempted to call airline to report attempted ATO. Call centre staff did not know how to respond and said they would have someone call. Never had a call back. As no points were taken I self-managed and monitored the account."

Conclusions

In our increasingly digital world, where everything – especially our loyalty programs – seems to be online and account-based, cybersecurity is paramount. Sadly, fraudsters are increasingly targeting loyalty programs, as witnessed by the escalating number of ATOs.



With brand trust and customer loyalty at stake, a single breach can cause lasting damage for airlines, like flyers never flying with them again. In an Arkose Labs report, 86% of airlines cited brand reputation loss as the top negative consequence from threats such as account takeovers, loyalty point theft, bonus abuse and inventory hoarding they've experienced over the past two years. And the financial stakes are high: the airlines also reported that due to the negative consequences, their losses reached up to $500 million over the past two years.

This straw poll, consistent with more detailed consumer research, indicates that around 5% of loyalty program respondents have experienced an account takeover. With 50% of those victims having had value removed from their accounts (ranging up to $5,000 USD), staying ahead of the fraudsters has never been more critical.

Following the LSA mantra:

Prevention:

Utilize cutting-edge cyber tools and robust program designs to prevent fraudsters from taking over accounts.

Detection:

If prevention is breached, ensure the program can detect the compromise at an account level immediately and halt the fraud in its tracks.

Communication & Recovery:

Implement a clear communication plan and efficient process for looking after your members post-compromise, prioritizing seamless recovery.

As Qantas, despite its significant cybersecurity investments, has recently shown, it is a matter of when, not if, your program will face a corporate-level breach. This is in addition to the relentless daily ATO risks that are happening constantly. Our collective vigilance and proactive measures are the only way forward.

Methodology

The Loyalty Security Alliance and Arkose Labs jointly designed the survey instrument to understand the impact of loyalty point fraud and theft on consumers and companies. LSA, along with its parent company, Airline Information Group Inc., sent the short survey to a sample of its database during February to June 2025. Short surveys were sent and delivered to 864 people in a spread of countries across the world. The database includes individuals who are frequent travelers and therefore likely to be members of loyalty programs. In addition, the database comprises professionals involved in various functions within the airline and travel industries, including loyalty security. This short survey approach is designed to be a "straw poll," and its aim was to gather a snapshot of those who might have had their loyalty program accounts compromised. For respondents who confirmed their accounts were taken over or compromised, additional questions were asked to ascertain the approximate value stolen (in US dollar terms). Furthermore, questions explored how victims discovered their accounts had been compromised and how their respective loyalty programs handled these fraud incidents.

Michael Smith

Michael Smith is one of the first people to work with Loyalty Programs to mitigate fraud, leading him to co-found the Loyalty Security Alliance. He is also currently a Board Member of Airline Information, a conference organiser for the Airline & Travel Industry specialized in sharing best practices in Loyalty Marketing, Fraud Prevention and Payments. Michael began his career in banking and prior to his current roles was a Board Director of British Airways Global Financial Services Limited. This included responsibility for developing mileage sales with partners such as American Express, Avis Car Rental and InterContinental Hotels and Resorts. He is based in Glasgow, Scotland, where he graduated with an MBA from the University of Strathclyde, as well as having professional qualifications in Marketing from the UK's Chartered Institute of Marketing.

Frank Teruel
COO
Arkose Labs

Frank Teruel is the Chief Operating Officer of Arkose Labs, the leading global account security company. At former companies, he has held GM, SVP, and COO positions, reflecting the breadth of his business acumen and leadership experience. Frank has spent the majority of his career leading Silicon Valley public and private technology companies in the digital identity, anti-fraud, and cybersecurity space, dedicating more than 20 years to helping the world's largest enterprises detect and prevent fraud and cybercriminal activity and ensuring trustworthy consumers have seamless online experiences. He is known for building high-performing teams, driving value, and achieving material business outcomes. Frank was instrumental in the successful ThreatMetrix $830M all cash acquisition by RELX/LexisNexis Risk Solutions. His leadership style is built on a strong desire and ability to quickly develop a deep understanding of all facets of a company: product, market, customers, and sales cycle. Prior to Arkose Labs, he was the CFO for Mitek Systems (NASDAQ: MITK). Frank started his career at PwC. For the past 12 years, Frank has served as an adjunct professor at Santa Clara University in the MBA program, imparting real-world wisdom and helping to develop the next generation of business leaders.

About the Loyalty Security Alliance (LSA)

LSA was co-founded by Michael Smith and Chris Staab who run payment and fraud conferences for airlines and travel companies. It was set-up specifically to help teams in cyber security, loyalty programs and fraud prevention deal with these challenges. It provides independent help and advice covering all frauds and abuses faced by Loyalty Programs, including Account Takeover (ATO), promotional abuse, staff and other customer program frauds. More details can be found at www.LoyaltySecurityAlliance.com or by contacting Michael Smith or Chris Staab.

About Arkose Labs

Arkose Labs is the leading global account security provider offering a comprehensive platform that combines proprietary device identification, phishing protection, email intelligence, scraping prevention, API security and bot management. The world's leading consumer brands—including two of the top three banks, Microsoft, Meta, Roblox, etc.—rely on the company's unified platform to reduce customer friction while preventing account takeovers, fake account sign-ups and SMS toll fraud. Its Security Operations Center (SOC) provides actionable insights from an extensive cross-industry intelligence network, which monitors legitimate traffic and attack patterns across global enterprises. With unparalleled proactive support for internal security teams, Arkose Labs goes beyond conventional security by actively partnering with customers to sabotage attacker profitability and disrupt threat actor groups like Storm-1152. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America.

Contact:
Cassie Stevenson
Arkose Labs
Global Head of Brand, Content and Communications
c.stevenson@arkoselabs.com