OLIVER WYMAN | FORTER®

PROTECTING CUSTOMERS FROM LOYALTY FRAUD

Joshua Gilbert
Robert Mau

EXECUTIVE SUMMARY

How often do you check your bank or credit card balance? Daily? Weekly? Do you have alerts setup to keep you informed of account changes and activity? Probably so.

When was the last time you checked your air miles balance? How closely are you monitoring your hotel points balance? When and how would you know if your loyalty account was hacked?

The lack of attention to loyalty accounts makes them a prime candidate for fraudsters. Not convinced? Consider the following:

- Globally, consumers have saved nearly 48 trillion loyalty program points[1], with a value of $160 billion in the US alone.[2]
- Nearly 50 percent of merchants indicate that low organizational priority and/or lack of resources are preventing effective deterrence to loyalty fraud.[3]
- Loyalty fraud attacks are growing rapidly, up 89 percent year over year during the first quarter of 2019.[4]

As companies continue to bolster defenses against more traditional fraud types, criminals have expanded into new areas – and loyalty programs are a prime target. The current defenses against such vulnerabilities are outdated and ineffective. Merchants are still largely dependent on inefficient manual processes and narrow point solutions. Consequently, many organizations are at risk for reputational and financial damages.

It is time for a new approach, one that addresses the problem broadly through modern techniques combined with state-of-the-art tools.

---

1 https://thepaypers.com/expert-opinion/48-trillion-unspent-loyalty-points-a-unique-opportunity-for-merchants/772524

2 https://www.pymnts.com/today-in-data/2018/loyalty-programs-subscription-commerce-fraud/

3 Primary research conducted by Forter.

4 Seventh Fraud Attack Index.

THE GROWTH OF LOYALTY FRAUD

Loyalty programs have grown tremendously in the last decade, with memberships up from 2.6 billion to 3.8 billion from 2012 to 2016 alone[5], and are projected to increase to 5.5 billion in 2020. Airlines, hotel chains, and financial services are the most prominent loyalty providers, but programs are proliferating quickly across sectors, including quick service restaurants and retailers.

Companies offer these programs to create and retain their most valued customers, and with good reason. In an intensely competitive world, 22 percent of consumers shop exclusively with brands at which they participate in the loyalty programs.[6] Loyalty programs encourage and reward lifetime value and allow companies to better identify and serve their best customers.

Criminals have taken note of the popularity of these programs. As companies implement fraud protection efforts that make traditional fraud more difficult to perpetrate, fraudsters have shifted to lower hanging fruit. Forter's Seventh Edition Fraud Attack Index showed that attacks on loyalty programs increased 89 percent in the first quarter of 2019, compared to 2018.[7]

Loyalty fraud is driven by many of the same macro trends affecting other fraud typologies. **Data breaches** continue to make PII more readily available; in the first six months of 2019 alone, 3,800 data breaches exposed 4.1 billion records. Historically, this would lead to higher rates of "step-up" authentication. However, customers increasingly expect **frictionless experiences** across all components of the journey[8], creating additional challenges for program operators. Further complicating protection efforts, many customers access their loyalty accounts infrequently, making anomaly detection more challenging and "step-up" authentication a greater source of customer friction.

Most consumers do not regularly track the points they have earned or redeemed, making loyalty programs particularly alluring to fraudsters; bad behavior may (and does) go unnoticed and unreported. Forty-five percent of consumer loyalty accounts are inactive[9], and many merchants are not adequately protecting their loyalty programs.[10] This is significant, as many programs provide a currency as valuable and untraceable as cash. Fraudulent incidents and abuse to such programs can cause damage to brand reputation, and monetary losses to merchants and consumers alike.

---

5 2017 Colloquy Loyalty Census, page 17.

6 https://www.pymnts.com/news/security-and-risk/2018/loyalty-rewards-programs-digital-fraud-prevention/

7 Seventh Fraud Attack Index.

8 https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html

9 Bond, The Loyalty Report 2019, page 4.

10 Primary research conducted by Forter.

WHAT'S AT STAKE

The damage can take many forms. At minimum, fraudulent attacks on a loyalty program diminish their intended benefit. But there are other consequences.

- **Tarnished Reputation:** Loyalty program executives report that the biggest impact of loyalty program fraud is on brand reputation and the negative customer experience.[11] The primary goal of loyalty programs is to drive customer retention and enhance lifetime customer value. Fraud directly puts these objectives at risk.

- **Lost Growth and Foregone Revenue:** Those same executives further report that loyalty sign up abuse leaves them unwilling to provide new offerings (such as aggressive promotions) due to the risk of abuse or loss.[12] Additionally, protection efforts that create too much customer friction can lower sign up and adoption rates, further diminishing their benefit.

- **Direct financial losses:** The most immediate impact is direct financial loss. When accounts are breached and points are stolen, points are redeemed for goods and services at a cost. Further, when fraudsters redeem points, merchants replace the points that fraudsters steal, increasing the burden to the business.

LOYALTY FRAUD: ATTACKS FROM ALL SIDES

Globally, consumers have saved nearly 48 trillion loyalty program points[13], with a value of $160 billion in the US alone.[14] Co-Founder Peter R. Maeder of the Loyalty Security Association (LSA), notes "one of the problems the loyalty industry has is that the miles or the points that have accumulated in an account are not treated at their true value. Unfortunately, the programs, and even the account holders, don't protect them." [15]

11 Primary research conducted by Forter.

12 Primary research conducted by Forter.

13 https://thepaypers.com/expert-opinion/48-trillion-unspent-loyalty-points-a-unique-opportunity-for-merchants/772524

14 https://www.pymnts.com/today-in-data/2018/loyalty-programs-subscription-commerce-fraud/

15 https://www.pymnts.com/news/security-and-risk/2018/loyalty-rewards-programs-digital-fraud-prevention/

Among vulnerable industries, airlines are frequently targeted. With 4.37 billion passengers per year, there is an immense quantity of data for criminals to exploit. According to the LSA, one percent of today's redeemed miles are fraudulent — a $3.1 billion problem worldwide.

Fraudsters recognize the value of the accumulated points, and they have found creative ways to realize that value. Threat vectors are present across the customer journey, including:

Typology	Description
Account Takeover (ATO)	3rd party fraudsters gain access to legitimate customer accounts and use points to: • Redeem for gift cards, which are virtually untraceable • Purchase travel tickets in the account holder's name, then change the name to a third party after selling the ticket Further, merchants often save customer credit card details within customer profiles, meaning that ATOs can exploit both points and dollars
Sign Up Abuse/ New Account Fraud	• 3rd party fraudsters open illegitimate accounts, often leveraging stolen identities to liquidate points from member accounts • Most commonly, fraudsters transfer points to a newly created account with the aim to sell them • Fraudsters also use fake accounts to earn and redeem points tied to stolen credit cards
Policy Abuse	• This type of activity is frequently perpetrated by legitimate customers • Thinking of themselves as "savvy shoppers," consumers will overshare coupon or promotional codes, thereby breaching merchant policies • Likewise, online fraudsters abuse coupons or referrals to gain access to financial payouts or valuable items or services

Insider abuse represents an additional threat vector, in which employees or others with privileged access to information or systems aid or perpetrate fraud. At the 2019 AFCE Fraud Conference in the Middle East, Amir Mousa of Al Ain Holding Group shared an instance of an employee who created loyalty accounts for customers, but used his own email address for each account, allowing him to accumulate 2.6 million air miles.

CHALLENGES WITH CURRENT APPROACHES

Forty-two percent of merchants report they do not have the skills internally to prevent fraud and abuse. Nearly 50 percent of merchants indicate that low organizational priority and/or lack of resources are the biggest barriers to preventing and deterring loyalty fraud. Fraudsters have noticed, and loyalty fraud attacks are growing rapidly, up 89 percent year over year during the first quarter of 2019. This puts customer loyalty, long term value, and merchant bottom line at risk.

Current approaches to loyalty program fraud management are insufficient, relying on:

Manual Review: Teams of people conduct ad hoc reviews using tools developed in-house that require repetitive, inefficient, and ineffective investigations.

Challenge: This approach is not scalable. It creates friction and frustration for customers. Many merchants use CRM systems to look for anomalies. In-house and other tools typically solve point-specific problems, but do not share information, creating siloes. Known fraudsters who attack at different customer touch points are therefore not noticed and able to slip through the cracks.

Manual reviews are subjective, less accurate, and less efficient. Most problematic, manual review is definitionally reactive. Review teams only see fraud after it occurs, rather than taking a proactive approach involving an automated system to detect and prevent fraud before it happens.

Point Solutions: Authentication at login only, assigning a score to interactions.

Challenge: By exclusively checking at login, merchants protect session integrity only at this specific point. Fraudsters can easily bypass this precaution, and then have free rein inside accounts. Further, risk scores are not actionable. They require complementary technologies or manual review teams to come to a decision.

THE WAY FORWARD

Legacy approaches that rely on large manual teams and point solutions are no longer fit-for-purpose. As fraudsters adapt, merchants need to innovate faster, staying one step ahead to protect their assets and customers' trust.

Are you ready to act to protect your most loyal customers? To address this challenge, merchants need a solution that:

- **Protects Consumers Throughout the Journey with an Integrated Platform.** To keep pace with the speed of change, merchants need to combine data, fraud detection capabilities, and machine learning into a single platform that can constantly be adapted and updated. This gives you a comprehensive view of all your customers – their interactions and behavior across the entire customer journey, not just on your site but on those of businesses across the globe. With this view, you can distinguish and protect your legitimate customers from fraudsters.
- **Delivers Decisions in Real Time.** Online shoppers expect instant gratification. With a competitive market of online brands to choose from, consumers will stay loyal to those and allow them to glide through to checkout. Risk scores and manual review of transactions add friction and delay purchase completion. A real-time fraud prevention platform means decisions, not scores. No guesswork. No manual steps that slow down your customers' online experience. Just accurate, instantaneous decisions to facilitate the buying journey.
- **Adapts to Your Business Requirements.** Your fraud prevention model requires continuous tailoring to ensure accurate decisions that meet your business model, risk appetite, service portfolio, the markets you operate in, and more. In ongoing partnerships where you provide feedback and business context, your fraud prevention solution will update and adapt to meet your unique business KPIs and fraud prevention requirements automatically – whether through peak periods, new service offerings, or business expansion.
- **Aggregates Data in a Global Merchant Coalition.** The platform must build a picture of consumer behavior that distinguishes fraudulent from legitimate activity by aggregating all merchant data across its network, not just the risky behaviors. The understanding of legitimate customer behavior allows you to increase your approval rates while minimizing fraud chargebacks.

Merchants have built loyalty programs to reward their most valuable customers. Online fraudsters have found these programs to be a treasure trove of opportunity. The time is now to invest in an enterprise-grade platform that delivers the most accurate decisions in real time to protect your most important asset: your most loyal and most valuable customers.

Oliver Wyman collaborated with Forter in the development of this point of view.

ABOUT FORTER

Forter is the leader in e-commerce fraud prevention, processing over $150 billion in online commerce transactions and protecting over 600 million consumers globally from credit card fraud, account takeover, identity theft, and more. The company's identity-based fraud prevention solution detects fraudulent activity in real-time, throughout all online consumer experiences. For more information please contact info@forter.com

ABOUT OLIVER WYMAN

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

Americas	EMEA	Asia Pacific
+1 212 541 8100	+44 20 7333 8333	+65 6510 9700