FORTER®

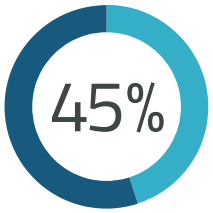
Loyalty Fraud: Attacks From All Sides

Produced in cooperation with
Loyalty Security Association

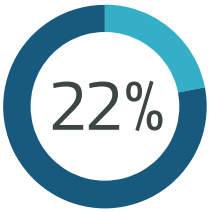
LSA
LOYALTY SECURITY ASSOCIATION

How often do you check your bank or credit card balance? Daily? Weekly? When was the last time you checked your air miles balance?

Forty-five percent of loyalty program accounts are inactive[1], merchants are not protecting their loyalty programs[2] — and fraudsters are taking note of these easy targets. They are increasingly shifting their attention to these accounts, which contain a currency as valuable and untraceable as cash, causing damage to brand reputation and monetary losses to merchants and consumers alike.



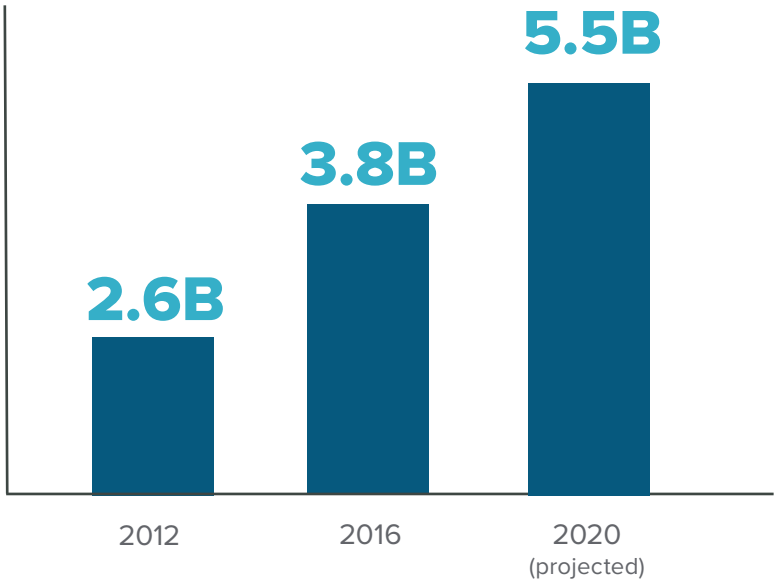
of loyalty programs accounts are inactive.



of consumers shop exclusively with brands of whose loyalty programs they are members.

Loyalty programs have grown tremendously in the last decade. Memberships rose from 2.6 billion to 3.8 billion from 2012 to 2016 alone[3], and are projected to increase to 5.5 billion in 2020. Retail, airline, and hospitality providers, quick-service restaurants, and financial services brands are the major players that offer these programs to their most valued and trusted customers. They do so with good reason: in an intensely competitive world, where rising customer expectations and frequent price promotions encourage consumers to switch to the best offer, 22 percent of consumers shop exclusively with brands whose loyalty programs they are members of[4]. Loyalty programs encourage and reward lifetime customer value.

Loyalty Program Memberships



Cyber-criminals have taken note of the popularity and growth of these programs and take advantage of them in several ways.

The most significant attack vectors include:

ACCOUNT TAKEOVER (ATO)

Fraudsters hack into member accounts, using the personal data and financial instruments therein.

NEW ACCOUNT FRAUD

Fraudsters create fake accounts, often using stolen identities, and use them to accumulate, store, sell, and redeem stolen points.

POLICY ABUSE

Consumers overshare coupons or promotional codes, violating merchant policies and illegitimately gaining program rewards.

Attacks on loyalty programs come from several sources:

FRAUDSTERS

Sophisticated professionals — whether lone attackers or those operating in fraud rings — monetize points associated with loyalty programs.

INSIDERS

Merchants' employees take advantage of their access to consumer accounts for any of the three attack vectors referenced above.

CONSUMERS

Considering themselves savvy shoppers, consumers misuse loyalty programs' policies to unfairly gain rewards.

Forter's Seventh Edition Fraud Attack Index showed that attacks on loyalty programs increased 89% in the first quarter of 2019 compared to 2018[5].

Inactivity in loyalty accounts, with consumers failing to track points they've earned or redeem those points, is one big reason that fraudsters find loyalty programs so alluring.

Data Breaches: Fueling e-Crime

JANUARY - JUNE 2019

3,800 Data breaches

4.1B Records exposed

The average impact of a data breach is a 5% drop in share price and a 7% loss of customer base[7]. These breaches coincide with hefty regulatory costs. Recent data breaches have cost large consumer-facing businesses GDPR fines of over £99 million ($123 million) and £183 million ($229 million)[8].

Fraudsters have discovered significant value within consumer accounts: personal, financial, shipping, billing, and other details. Consumers often use the same login credentials for many accounts, so when fraudsters breach one account, they have the keys to other accounts held by the same person, including their loyalty program accounts.

Even if you haven't suffered a data breach, you are likely to feel the effect when other merchants' programs have been attacked.

The increase in loyalty program fraud has been driven by the enormous amount of personally identifiable information that has become available via massive data breaches. In the first six months of 2019 alone, 3,800 data breaches exposed 4.1 billion records[6].

THE AVERAGE IMPACT OF A DATA BREACH

REGULATORY FINES ASSOCIATED WITH DATA BREACHES

£183M ($229M)

£99M ($123M)

The Impact is Widespread

The damage to enterprises takes many forms.

TARNISHED REPUTATION

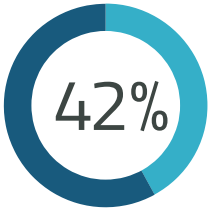
Loyalty program executives report that the biggest impacts of loyalty program fraud are on brand reputation and customer experience[9].

LOST REVENUE

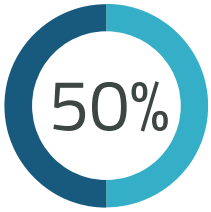
When fraudsters redeem points, merchants replace the stolen points, doubling the loss to the business.

STIFLED BUSINESS GROWTH

Those same executives further report that loyalty sign-up abuse leaves them unable to provide new offerings, such as aggressive promotions or gift cards, due to the risk of abuse or loss[10].



of merchants report that they do not have the skills internally to prevent fraud and abuse[11].



of merchants indicate that low organizational priority and/or lack of resources are the biggest barriers to preventing and deterring loyalty fraud[12].

It's clear that loyalty programs are ripe for the taking.

The resulting shift of fraudster attention from pure transactional credit card fraud to these programs puts customer loyalty, long-term value, and your bottom line at risk.

Loyalty Fraud: Attacks from All Sides

In part because of the growing success in fighting credit card fraud at the point of payment, fraudsters have shifted their focus to loyalty programs.

Consumers have saved nearly 48 trillion loyalty program points globally[13], with a value of $160 billion in the US alone[14]. Peter R. Maeder, cofounder 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]
>
> Peter R. Maeder
> Co-Founder, Loyalty Security Association (LSA)

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[16]. According to the LSA, 1% of today's redeemed miles are fraudulent — a $3.1 billion problem worldwide[17].

Fraudsters recognize the value of the accumulated points, and they've found creative ways to realize that value.

ACCOUNT TAKEOVER (ATO)

is an increasingly common attack vector in which fraudsters access genuine accounts. Once inside the account, fraudsters redeem members' points for rewards. They will redeem points for gift cards, which are an untraceable instrument. They will purchase tickets for travel in the account holder's name, then, after selling the ticket, change the name to that of a third party.

POLICY ABUSE

refers to fraudulent activity by otherwise good customers. Thinking of themselves as savvy shoppers, consumers will overshare coupons or promotional codes, which may be against merchants' policies. Likewise, online fraudsters abuse coupons or referrals to gain access to financial payouts or valuable items or services.

NEW ACCOUNT FRAUD

gives fraudsters an opportunity to liquidate points they've stolen from legitimate member accounts. They create multiple fake accounts, occasionally leveraging stolen identities, and use them for a variety of schemes. Most commonly they transfer the points to a newly created account with the aim to sell them[18], in many cases to a fake account set

up by the fraud ring, or to other third parties who use the points to purchase goods or services. Fraudsters also use fake accounts to earn and redeem points tied to stolen credit cards.

INSIDER ABUSE

sees even employees get involved in the action, using any of the above referenced tactics, since they have access to customer accounts and personal details. 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[19].

It's time to act.

Challenges with Current Approaches

Current approaches to loyalty program fraud prevention are not sufficiently robust. Competing priorities — the need to deliver a frictionless user experience to maintain customer lifetime value versus the cost of fraud prevention as compared to the perceived risk, and the need to deliver new products and services to remain competitive — make it challenging to secure buy-in and investment for improving fraud detection capabilities[20].

Current methods of fraud prevention include some combination of:

Manual Review or Fraud Teams

This approach relies on large teams of manual reviewers who are supported by tools developed in-house.

PAIN POINT

This approach is not scalable. It adds friction and frustration for customers. The time it adds to a transaction, especially for items such as travel or event tickets, for which prices change quickly, can cause consumers to abandon transactions. The need for seasonal workers to handle high-volume periods such as holidays imposes significant costs and adds workers with less training and experience.

Manual review teams only see fraud after it occurs, rather than taking a proactive approach and training an automated system to prevent fraud before it happens.

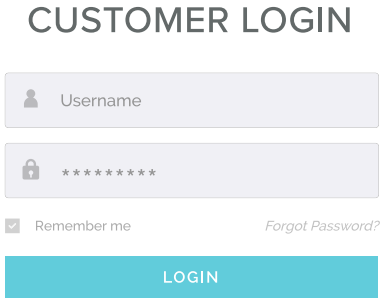
Today between **40 and 50 percent** of organizations conduct fraud capabilities internally[21].

Single Point Protection

Authentication at login only, assigning a score to interactions

PAIN POINT

By looking only at login, merchants protect session integrity only at this specific point. Fraudsters can easily bypass this precaution and then have free rein inside accounts they've entered[22]. Further, risk scores are not actionable. They require complementary technologies or manual review teams to come to a decision.



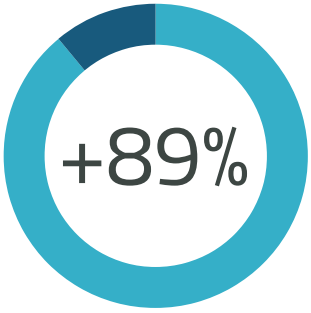
The Way Forward

Loyalty program fraud affects the very customers most important to a business: your best and most loyal customers. The number of loyalty program accounts grows consistently year over year. With so many of those accounts inactive, there is a very large and untapped asset that merchants and enterprises are not prepared to protect.

Fraudsters have noticed, and loyalty fraud attacks are growing rapidly, up 89% year over year during the first quarter of 2019[23].

Fraud is shifting. Fraudsters are attacking across all points of the customer journey, no longer only at the point of the transaction. They are opening fake accounts to redeem stolen points. They are abusing policies, inhibiting merchants from launching new promotions.

Loyalty Program Fraud Attacks



from first quarter 2018 - 2019

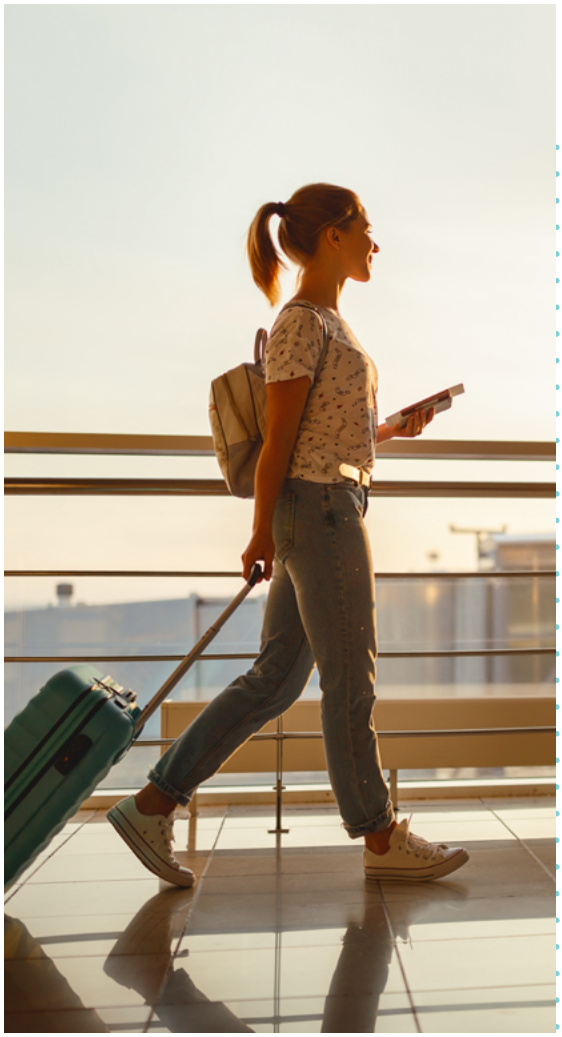
Legacy methods that rely on large manual review teams and solutions that focus on specific interactions do not share information sufficiently to find and prevent fraud and abuse before it occurs. Merchants are afraid to create new programs or products due to perceived risks. And they don't prioritize resolving this.

Are you ready to act to protect your most loyal customers?

To address this challenge, technology must:

PROTECT CONSUMERS THROUGHOUT THE CUSTOMER JOURNEY

To keep pace with the speed of change, you need to combine data, fraud detection capabilities, and machine learning into a single platform that can constantly be adapted and updated. You thereby leverage a comprehensive view of all your customers and their interactions and behavior across the entire customer journey, not just on your site but on those of businesses across the globe. You'll be able to distinguish and protect your legitimate customers from fraudsters.



DELIVER REAL TIME DECISIONS

Consumers expect instant gratification. With a competitive market of online brands to choose from, consumers will stay loyal to brands that trust them and allow them to glide through to checkout. Risk scores and manual review of the riskiest transactions add friction and delay completion of the transaction. 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 that don't get in the way of the buying journey.

ADAPT TO YOUR BUSINESS REQUIREMENTS

Your fraud prevention model requires continuous tailoring to ensure accurate decisions specific to your business model, your risk appetite, the markets you operate in, and more. As your business evolves, your fraud prevention solution will update and adapt to meet your unique KPIs and fraud prevention requirements

AGGREGATE 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 value, since merchants are not prepared to protect these programs and customers don't check their account balances frequently.

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.

For more information, visit **forter.com**.

[1] Bond, The Loyalty Report 2019, page 4.
[2] Forter primary research, October 2019.
[3] 2017 Colloquy Loyalty Census, page 17.
[4] https://www.pymnts.com/news/security-and-risk/2018/loyalty-rewards-programs-digital-fraud-prevention/
[5] Seventh Fraud Attack Index.
[6] https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html
[7] https://www.centrify.com/resources/the-impact-of-data-breaches-on-reputation-and-share-value/
[8] https://www.forbes.com/sites/kateoflahertyuk/2019/07/09/marriott-faces-gdpr-fine-of-123-million/#9618dd045253
[9] Forter primary research, October 2019.
[10] Forter primary research, October 2019
[11] Forter primary research, October 2019.
[12] Forter primary research, October 2019.
[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/
[16] Statista, "Number of Scheduled Passengers Boarded by the Global Airline Industry from 2004 to 2019," August 9, 2019.
[17] https://securityintelligence.com/why-fraudsters-are-flying-high-on-airline-loyalty-programs/
[18] Secure Loyalty Program Accounts from Fraud to Preserve Customer Trust. (Gartner) pg 3
[19] https://www.fraudconferencenews.com/home/2019/2/25/how-to-stop-fraud-in-loyalty-programs
[20] Secure Loyalty Program Accounts From Fraud to Preserve Customer Trust. (Gartner) pg 7-8
[21] Forter primary research, October 2019.
[22] Secure Loyalty Program Accounts from Fraud to Preserve Customer Trust. (Gartner) pg 4
[23] Seventh Fraud Attack Index.

FORTER®

Web: https://forter.com | Email: info@forter.com | EMEA: emea@forter.com | APAC: apac@forter.com

ABOUT FORTER

Forter is the leader in e-commerce fraud prevention, annually protecting over $150 billion in online commerce transactions for over 500 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. Forter's integrated fraud prevention platform is fed by its rapidly growing Global Merchant Network, underpinned by predictive fraud research and modeling, and the ability for customers to tailor the platform for their specific needs. As a result, Forter is trusted by Fortune 500 companies to deliver exceptional accuracy, a smoother user experience, and elevated sales at a much lower cost. Forter is backed by $100M of capital from top-tier VCs including Sequoia, NEA, and Salesforce.

https://www.forter.com

Produced in cooperation with
Loyalty Security Association