BRING ON
THE FUTURE

Kaspersky
Fraud Prevention

Kaspersky Fraud Prevention for loyalty programs

Loyalty schemes have not only become pivotal in increasing sales and achieving great returns on investment but also in establishing a mutually beneficial relationship with the customer. Ensuring that a customer's benefits, bonuses and points are protected is key to building loyalty.

Some facts and statistics

Over **$100 billion** a year in loyalty points fail to be redeemed, according to Bond Brand Loyalty.[1]

Almost half (**45%**) of users aged 18-34 prefer using their mobile app to redeem bonus points.[2]

Accounts with up to **50.000** travel miles can be sold for as little as **$90** on the DarkWeb.[3]

Organizations with loyalty programs face tough consequences when they encounter fraud:

- Restoring stolen points and loyalty program benefits to victims
- Recovering their brand reputation
- Keeping the consumer within the loyalty program

Overview of the field

No matter the size of the organization, modern consumers have become extremely accustomed to rewards, bonus points and loyalty programs.However, loyalty programs have become extremely attractive to fraudsters, with many seeing them as "the path of least resistance".

New marketing promotions and bonus redemption landing pages attract fraudsters looking to profit at the expense of loyalty programs. The more intricate, complex and widely advertised these programs become, the more likely they are to be prone to fraud.

The Kaspersky Fraud Prevention Team recently discovered over 3,000 fake accounts in the loyalty program of just one major retailer. These accounts were used to acquire welcome bonuses for newly registered users, and were then sold on the dark web at a reduced fee.

Why are fraudsters attracted by loyalty programs?

The fraudsters are lured by the hefty unspent budgets that companies invest in the promotion of marketing campaigns. For example, Starbucks reported $1.6 million of unused funds on their customer loyalty cards. These trends have been becoming more and more prominent, attracting fraudsters looking for easy targets.[4]

Moreover, the design of loyalty programs introduces multiple vulnerabilities throughout the whole customer journey, making it harder to protect using two-factor authentication. To avoid fraud, protection needs to be present at all touch points – from the user logging in and signing up for the bonus program to redeeming their reward.

Customers tend to be less aware of their balance and the amount of bonus points they've accumulated, as well as being less informed about loyalty fraud in general. All these factors combine to create an easy pathway for fraudsters to abuse loyalty programs.

Ensuring an organization does not suffer financial and reputational consequences requires strong yet seamless authentication and analysis of both identities and sessional data. Striking a balance between the protection of customers from new account fraud and account takeover, while ensuring the user experience is seamless and smooth remains a key challenge.

However, with the right fraud prevention solution many of these issues can be overcome thanks to the ability to recognize legitimate customers. This can be achieved with machine learning tools capable of identifying synthetic accounts that are created to accumulate bonus points and benefit from loyalty programs.

[1] The 2017 Bond Loyalty Report
https://info.bondbrandloyalty.com/the-2017-bond-loyalty-report-press-release-us
[2] Loyalty One LBP Report
https://storage.pardot.com/223662/91321/190023_LoyaltyOne_LBP_Report_Final_Apr24.pdf
[3] Armor The Black Market Report 2019
https://www.armor.com/resources/reselling-hospitality-look-hotel-rewards-dark-web/
[4] Starbucks 2019 Annual Report
https://investor.starbucks.com/financial-data/annual-reports/default.aspx

Preventing fraud in loyalty programs

New account fraud

- Immediate recognition of synthetic accounts
- Detection of new unknown devices

Account takeover

- Uncovering signs of ATO at the stage of a login and throughout the session
- Detecting anomalies & suspicious behavior in real-time
- Accuracy and speed of detection

Kaspersky Fraud Prevention

Kaspersky Fraud Prevention helps organizations achieve that happy medium between usability and security of digital services. Backed by Kaspersky's 23 years of experience in cybersecurity, Kaspersky Fraud Prevention takes pride in helping service providers reach the pinnacle of protection. All this comes with flexible case management and forensic capabilities that significantly reduce operational costs for enterprises.

Kaspersky Advanced Authentication

- Prioritizing legitimate users and detecting suspicious ones
- Risk-based authentication continuously monitors numerous unique parameters
- Real-time analysis of biometric, behavioral and environmental data
- Legitimate users proceed to their digital accounts without any unnecessary verification steps, which means reduced two-factor authentication costs for providers

Kaspersky Automated Fraud Analytics

- Advanced machine learning makes sure all data and activity are monitored throughout the whole session
- Continuous detection and analysis of in-session events like bots, malware, remote administration tools, new unknown devices, web injects, and more
- Identification of new account fraud and account takeover incidents
- Global mapping, link building and device identification

Fraud research and analysis team

Continue the conversation with our analysts to learn how global threat intelligence and cutting-edge technologies combined will help you grow your business without security concerns and usability issues.

Beat fraud and ensure seamless digital experience for your clients. **Kaspersky Fraud Prevention**

True machine learning

Forensic capabilities

Reduced operational costs

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com

Kaspersky
Fraud
Prevention

Order your demo by contacting us at
kfp@kaspersky.com

More information at
https://kfp.kaspersky.com

@KasperskyFP