Maritz®

Keep Loyalty Programs Rewarding

Protecting Your Customers from Fraud

2025 EBOOK

Introduction

> "With over **$48 trillion of unspent loyalty points globally** it's no wonder malicious actors are targeting rewards programs globally..."

– 48 Trillion Reasons Loyalty Fraud is on the Rise, The Wise Marketer

Loyalty marketers have a lot on their minds: acquiring new members, keeping those members engaged, managing the return on investment – and then there's the ever-increasing risk of fraud.

Fraudulent access to customer accounts continues to grow and the cost is significant. With the cost estimated at $1 Billion annually, businesses must find effective ways to protect their loyalty programs and their customers.

While challenges like internal fraud and customers "gaming the system" need to be addressed, the real danger is external fraud. Loyalty marketers need to understand how it happens and what to do about it.

Types of External Fraud

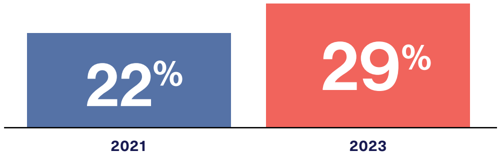
The Loyalty Security Alliance describes these four types of external fraud:

- Account Takeovers
- Identity Theft
- Social Engineering
- Botnet Attacks

According to the Association of Certified Fraud Examiners, the most common type of fraud is Account Takeovers - where the fraudster gains access to your customers' accounts and makes unauthorized transactions.

Account Takeover Has Increased Since 2021

% of People Who Have Had An Account Taken Over Through Sign-On Credentials



Account takeover is just what it sounds like: In loyalty programs, fraudsters literally take over customers' loyalty accounts to steal and redeem points for rewards (such as merchandise, travel, and gift cards), which they can readily turn into cash.

And that's not the only thing they're after. Andrew Kunesh, a.k.a. The Points Guy, says they can also gain data to build profiles on your customers – information that can be sold on the darknet.

When this kind of fraud occurs, what's meant to reward customer loyalty and ultimately increase your revenue can become a liability, both financially and to your brand's reputation. The good news is that most loyalty program transactions go through without incident. By taking advantage of ever-evolving tools and processes to prevent and detect fraud, you can improve your odds of successfully stopping it.

A survey conducted by Security.org in 2023 showed that the percentage of American adults who have experienced account takeover in their lives has risen to 29%, which equates to **77 million adults** – an increase from 22% in 2021.

How Bad Actors Take Over Accounts

The Loyalty Security Alliance also reports that account takeover typically depends on the bad actors gaining access to customer accounts in one of the following ways:

Credential Stuffing

This occurs when bad actors obtain large quantities of usernames and passwords as part of a larger data breach. Since people tend to use the same login credentials across multiple accounts, the fraudsters copy and paste those credentials into other websites. Tools like AI are making this even easier.

Social Engineering/Phishing

Fraudsters often create authentic-looking links and landing pages, tricking users into providing their login credentials.

Malware

Commonly installed through a phishing attack, malware can do things like record keystrokes when you login, copy credentials when you enter them, or even provide remote access directly into to your computer.

Session Jacking

Fraudsters can hijack an active user's session by intercepting and stealing an active session token. The token grants them direct access into the account – and then they can do all the things the user can do, like redeeming loyalty points for valuable rewards.

Balancing Fraud Reduction vs. Friction Reduction

Like it or not, customers expect companies to help protect them from fraud and cover any losses if it occurs. Adding additional verification steps at login helps make it harder for fraudsters to take over accounts, but those same customers want the online experience to be "frictionless." So, what's more important?

It depends on your customer's sensitivity to friction and your company's tolerance for risk. Regardless, you need to strike the right balance for your program. Communicating what you are doing to reduce fraud, and the reasons for any extra verification steps is part of the answer. Making sure you're doing all you can to prevent fraud is the other.

Preventing Account Takeovers

There are several things loyalty program owners can do to minimize the chances of fraud:

Work with your technology and fraud protection teams.

Collaborate to put the right tools in place to increase security, prevent attacks and quickly identify and address attacks when they occur.

Always alert users when a data breach occurs.

When notifying your customers, instruct them to not only deal with potentially compromised credit card data, but to also carefully check their loyalty points as well, and remind them to change their passwords.

Educate customers on how to keep their accounts secure.

Encourage people to frequently check account balances, change passwords and use unique passwords for different accounts.

Require employees to take precautions.

Bad actors love to take advantage of lax data protection practices. Provide regular security training across your organization and require employees to change their passwords using strong, unique variations for each of their accounts. Limit access to sensitive data to only those who need it.

Use additional and up-to-date security measures.

Multi-factor authentication, tokens and biometrics are some to consider, but improvements and updates are ongoing. Be sure your technology team keeps your employees and customers up to date.

Be sure your partners take the same care you do.

Loyalty marketers often rely on outside partners for aspects of their programs, such as technology providers to manage point calculations and point banks, and reward providers to provide additional redemption options. A strong partnership between your technology and fraud teams, as well as those of your partners, is essential. Your reward redemption partners are a last line of defense, so understand their capabilities to catch and address fraudulent orders.

Stopping Fraud at Redemption

What can you do when a bad actor successfully takes over accounts and redeems for rewards? If you have the right reward partner, it's possible to catch those orders and cancel them before they are fulfilled.

Technology Tools and Data

While bad actors' techniques have become more sophisticated, the technology to mitigate fraud has also evolved.

Some tools inspect the data from the devices accessing the rewards website and identify threats and anomalies. Other tools use machine learning to spot potential fraud by analyzing comprehensive details about the online user's identity and behaviors. Pre-determined rules look at variables such as order value, email and shipping addresses, device used and order frequency.

With the right tools, incoming orders can be given a "fraud score" to indicate a likelihood that the order might be fraudulent and trigger next steps to prevent fulfillment from going through. The higher the score, the more likely it's a fraudulent order. Over time, as more data feeds into these tools, the more the tools learn and improve the accuracy at detecting potential fraud.

People and Process

Scoring and identifying potentially fraudulent orders is just the first step – but what do you do now? Now you need to get people involved and develop the right processes.

Typically, high scoring orders are canceled and flagged as fraudulent, low scoring orders are fulfilled, and mid-scoring orders are placed "on review." This is where you want to make sure your reward provider has experienced people working with you – both their fraud team as well as a project manager that works with your program daily.

While tools and technology are great, they're looking at data and patterns that have happened in the past. Reward fraud experts can sometimes identify patterns that the technology doesn't notice or hasn't yet learned to spot. Examples include a project manager noticing a series of disparate orders with the same email address or finding several orders with slightly different spellings of the same street name.

Identifying patterns like this can also be used to bounce against low scoring orders that the tools didn't detect and stop even more fraud. Sometimes, when reviewing orders, people just have a feeling that something is off, and they're typically right. Since fraudsters and their techniques are always evolving, and tools and technology take time to catch up, the human element becomes a critical part of the fraud prevention process.

Collaboration and Mutual Trust Make the Difference

It's important that people at both your company and the reward provider collaborate closely to not only develop processes and procedures, but also continually evolve them to stay ahead of new fraud schemes.

Over time, as both teams work together, they have a much better chance at developing new approaches that will improve the chances of mitigating fraud. You want to make sure your reward provider is as diligent as you are about protecting your customers and your brand.

A Fraud Protection Checklist for Choosing a Rewards Provider

When considering new or existing providers be sure to ask the following questions to make sure they're doing all they can to protect your program and your customers:

- Does the provider have experience with programs that are like yours, especially in terms of volume and complexity?
- Is there a dedicated and experienced fraud team that includes both project management and technology team members to detect and deal with fraud?
- Can the partner point to examples of their ability to collaborate and solve more difficult examples of fraud?
- Do they have strong data security requirements such as ongoing training and enforcing strong passwords to ensure bad actors can't break into your data through employees?
- Is the customer service team and all individuals who may work with your orders or customers trained in how to spot fraud and handle situations quickly and professionally?

Avoid the Financial and Reputational Risk of External Fraud

Of course, there is a lot to think about as a loyalty marketer. External fraud aimed at your loyalty program is a big part of that. But with the right tools, processes and partners, you can minimize the financial and reputational risks of fraud directed at your program.

Contact us

Reach out to Maritz to learn more about reward strategies and solutions that help you enhance your loyalty program and engage your customers while also reducing your risk for fraud.