VOLUME 1, 2020

LSA BEST PRACTICE GUIDE

LOYALTY FRAUD

LSA
LOYALTY SECURITY ASSOCIATION

TABLE OF CONTENTS

INTRODUCTION

When we founded the Loyalty Security Association, as the LFPA in 2016, it was in answer to a need in the Loyalty Industry. A need for information, advice, and help combatting Loyalty Fraud.

Loyalty and Payment Fraud hurt merchants of all types. The card payment industry realized long ago that they were fighting a common enemy and joined forces to develop and introduce tools and solutions to make card transactions more secure.

This led to a change in how fraudsters behaved, they now focused more on Loyalty; a field where the opportunities for a significant return on limited effort were wide open.

After all, the Loyalty Programs are on their own – there is no overriding body that defends their interest. No industry standard, yet, in defining the types of fraud, no set procedures or rules to live by, which leads to a struggle in limiting loyalty fraud losses.

The LSA offers a platform for Loyalty Programs to meet with their counterparts to discuss ways to reduce fraud, find providers with solutions, and start setting standards whilst sharing Best Practices.

Our event participants have requested us to develop a Best Practice Guide, and we are doing so with the help of industry experts. They will contribute their know-how in specific areas, with examples and guidelines, tips and advice.

We are publishing these chapters, rolling them out one-by-one for now, and bundling them in the future. It is the LSA's hope that you will not only enjoy reading these chapters, but most of all, find some useful information in them to take away and implement.

If you would like to contribute to our Guide or have a topic you would like to see included, let us know, we are in this together after all.

PETER MAEDER
CO-FOUNDER, SECRETARY

Loyalty Fraud: The Basics

What is a Loyalty Program?

A Loyalty Program is a marketing tool designed to keep customers coming back. In exchange for their "loyalty" to your brand, product, or services, they are rewarded with discounts, freebies, and perks.

Unfortunately, there are some people who do not play by the rules to attain these rewards – this is called Loyalty Fraud.

In This Volume

What is Loyalty Fraud?

One of the biggest problems in Loyalty Fraud is the lack of a formal definition.

Loyalty Programs rely on points or rewards, instead of straight monetary restrictions, which means there is not a high level of scrutiny as there is in other aspects of sales, such as credit cards. The average customer doesn't track their loyalty points very well until they are ready to use them.

As such, most Loyalty Programs don't benefit from strong data security. This leaves a weakness that attracts criminals and thieves. Though most programs don't normally involve monetary transactions, stolen points are as good as cash if those rewards can be redeemed for hotel stays, airline tickets, or other high value items.

In contrast, credit card and payment fraud cases are well defined, have legal regulations, and use well-established detection and prevention methods, all of which are widely understood. Organizations struggle to provide a universal explanation as to what Loyalty Fraud is as it can vary depending on how a loyalty program is structured and how customers are rewarded.

Instead of trying to come up with a generic definition that would cover all possible fraudulent activities, it is first necessary to distinguish the most common types of Loyalty Fraud by establishing what parties are involved, and the motivation behind the fraudulent action.

THREE COMMON TYPES OF LOYALTY FRAUD

There are several categories of Loyalty Fraud, including:

1

Internal Fraud

Fraud committed by internal actors such as site staff, program administrators, Contact Center agents, partners, and integrators, exploiting their “insider” privileges against the program’s Terms & Conditions.

2

External Fraud

Organized, hostile actions by external actors. This is fraud in the form of Account Takeovers, identity theft, social engineering, and botnet attacks.

3

”Gaming” Fraud

Also called “Friendly Fraud,” this is fraud committed by a member or a user who is exploiting a loophole for personal advantage. Think of accrual loops, unauthorized redemptions, promotion abuses, integration flaws or process misconfiguration.

As you can see from this short list alone, departments other than the Loyalty department need to be involved with fighting Loyalty Fraud.

Other departments include:

- HR (internal fraud)
- IT (bot protection, multi factor login, secured information storage)
- Legal (loopholes, Terms & Conditions)
- PR who should have a “worst case” scenario plan ready to communicate with customers if something happens.

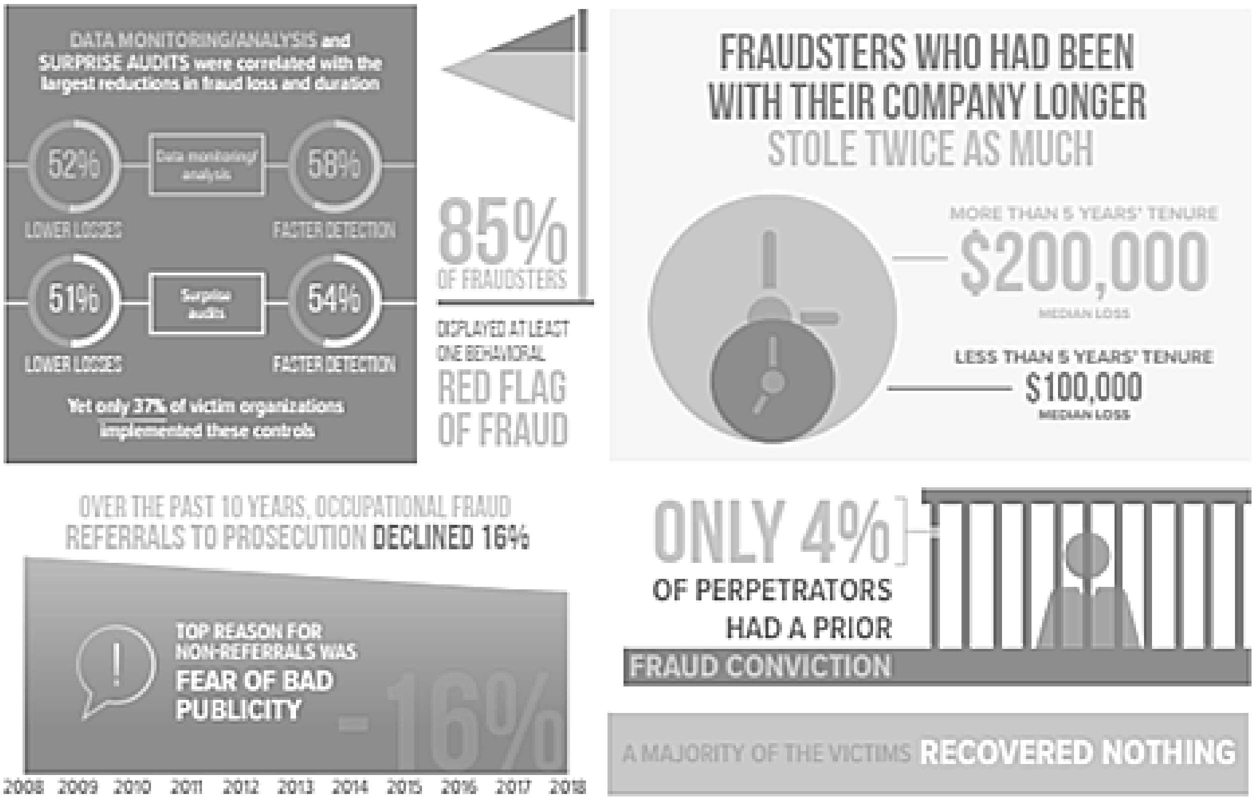
Buy-in and support at senior management level is key to this sort of cooperation between departments .

Internal Fraud

Security teams assigned to create and maintain procedures to protect loyalty programs tend to focus solely on external threats, while oftentimes, the biggest risk lies within the organization itself. At the end of the day, it is the people that keep the loyalty scheme running – administrators, analysts, customer service agents, and site staff – that cause a much higher risk than external bad actors. Realizing the risks by outsiders, most organizations often overlook insiders as potential bad actors.

Internal Fraud is a growing concern, especially considering that customer service related to loyalty is commonly outsourced. Coupled with a relatively high rate of staff turn-over, contact centers and customer support operations need to be under on-going scrutiny with proper reporting procedures in place and escalation paths clearly defined.

Additionally, implementing basic workflow mechanisms where, for example, the contact center supervisor must approve certain risky operations (such as manual points corrections or big point transfers), can be a simple but effective way for reducing the risk of internal fraud.



Source: ACFA 2018 GLOBAL STUDY ON OCCUPATIONAL FRAUD AND ABUSE

EXTERNAL FRAUD

External fraud includes the types of fraud that first come to mind when we hear the word. Simply put, it's an attack from an outside agent. This can be done in various ways. Some of the ways external fraud can be carried out include:

- **Account Takeovers** – ATO is a form of identity theft in which the fraudster gets access to a victim's accounts — through a data breach, malware, or phishing — and uses them to make unauthorized transactions.

- **Identity Theft** – Similar to ATO, but in an ATO, the criminal is using an existing account, whereas under identity theft, they use the same information to create a new account, pretending to be the victim.

- **Social Engineering** – Social engineering is the act of manipulating people so they give up confidential information, whether this is through phishing emails, vishing (VoIP "phishing) calls, malware (usual installed covertly after a "baiting" offer of, for example, a movie download), pretexting, or other means.

- **Botnet Attacks** – A botnet is a network of compromised - infected with malware - computers that can overtake a network. An attack can be anything from credentials leaks, unauthorized access, data theft, or DDoS attacks.

"Gaming" Fraud

Gaming Fraud is an ambiguous category – some see it as obvious Fraud, and others see it as a gray area. In gaming, a Loyalty Program member attempts to "game the system" by taking advantage of the Terms & Conditions or the system's loopholes by double-dipping, attaching their reward account to purchases they didn't make, status-matching infinitely from one program to the next, bartering points, or other means. .

- **Double-dipping** – A program member attempts to redeem points both online as well as on the phone with a representative, or gaining points illegitimately for the same activity in two different Loyalty Programs by whatever means.

- **Purchases Not Made** – The member books a room in their name and attaches their loyalty number, but someone else is staying in the room and paying for it. Most programs only allow earning points if the member is actually staying in the room.

- **Status Match** – A status match (or status challenge) is a shortcut opportunity to qualify for elite status with a program without actually holding that, or any, status, or being eligible to. Some programs intermingle matching between airlines and hotels. Most offers can be redeemed once within the lifetime of the membership, or for a limited time (i.e. some airlines allow status matching every 3 years). A gamer can traverse a status match from one program to the next to the next and on.

- **Brokering (bartering)**– Though programs allow members to gift points or awards, selling them, which is often referred to as "Brokering", is often prohibited by the program's policy.

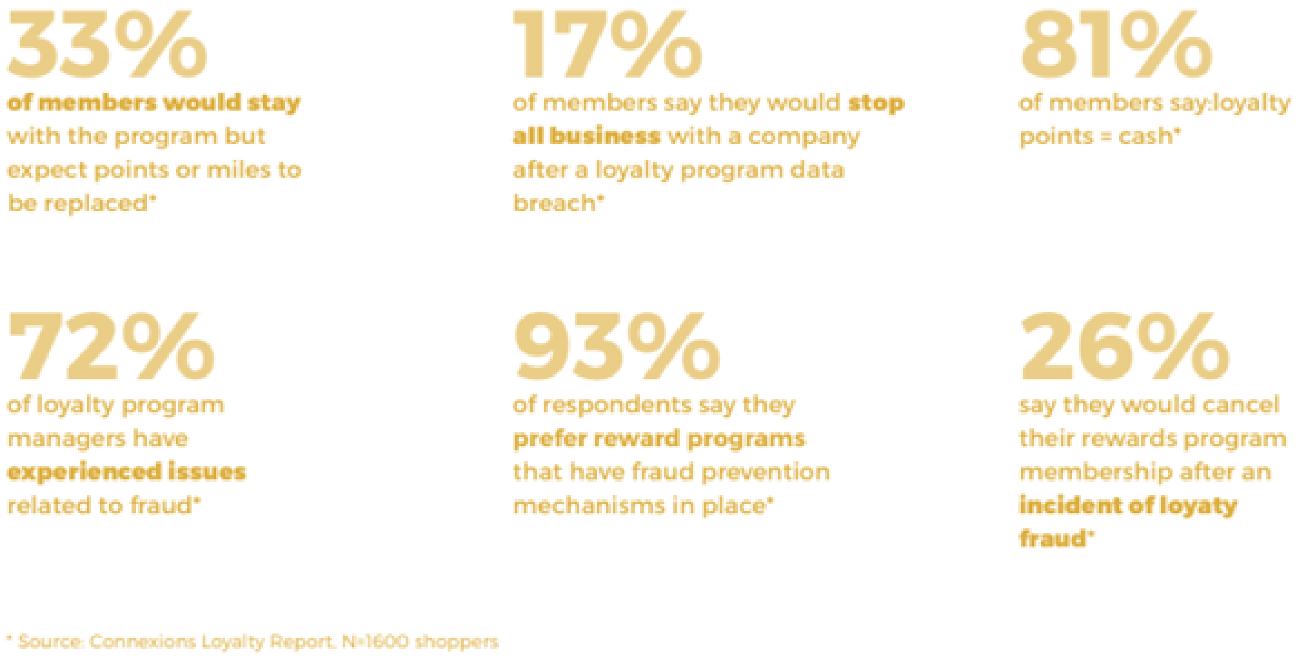
QUANTIFICATION OF THE LOSSES FROM LOYALTY FRAUD

A very common issue many companies face is assigning a hard-monetary value to the losses from loyalty fraud. Without a bottom-line universal loss metric, it is difficult to justify loyalty fraud expense and persuade senior management to invest in loyalty security. How can businesses create a dedicated fraud prevention team if we cannot analyze the cost-benefit?

There is no single solution to this challenge, but answering the following questions may help:

- What is the price per point in the program?
- Is there a formal points/rewards billing mechanism in place?
- What is the estimated member acquisition cost?
- Are the program's costs centralized or distributed across sites and partners?
- What is the average Customer Lifetime Value for loyalty members?

Along with analyzing the answers to these questions, it is important to consider the following statistics:



33%
of members would stay with the program but expect points or miles to be replaced*

17%
of members say they would **stop all business** with a company after a loyalty program data breach*

81%
of members say:loyalty points = cash*

72%
of loyalty program managers have **experienced issues** related to fraud*

93%
of respondents say they **prefer reward programs** that have fraud prevention mechanisms in place*

26%
say they would cancel their rewards program membership after an **incident of loyaty fraud***

* Source: Connexions Loyalty Report, N=1600 shoppers

LOYALTY FRAUD PREVENTION TIPS:

- Examine your current rewards program for any potential loopholes.

- Limit employee access to all loyalty program data on a strictly need-to-know basis. This approach is known as the principle of least privilege, and can help reduce the likelihood of loyalty points falling into the wrong hands.

- Have everyone on your team use strong (and unique) alphanumeric passwords for each of their accounts. If possible, you should set up your website so that customers are **required** to use secure passwords.

- Always alert users when a data breach occurs. In the aftermath of a breach, most businesses, banks, and victims focus on potentially compromised credit card data. When notifying your customers, instruct them to carefully check their loyalty points as well.

- Enable at least two-factor authentication (2FA) for all logins, or use other multi-factor authentication — both for your employees and for your customers. Thieves can easily get their hands on one piece of information (like a password), but it's much harder for them to gain access to mobile devices or guess people's high school mascot.

- Tokenize everything. This data security method is normally used to protect payment information — like credit card numbers, but can be used for any piece of data, including usernames, passwords, and email addresses.

SUMMARY

Loyalty Fraud encompasses more than most people assume, which means getting departments to work together to prevent breaches, and detect attacks can be difficult, but it is nevertheless important. Management **must** be involved to ensure that this process runs smoothly.

Just because loyalty programs use “points” as their form of currency, that doesn’t mean they don’t have value – to both your customer **and** your company. Losing the confidence of your loyal customer can end up costing you more than the costs of implementing secure logins, investing in AI to scan for issues, and hiring staff that’s trustworthy.

This volume was written in
cooperation with

COMARCH

Founded in 1993, Comarch has over 25 years of experience in designing, implementing and integrating IT solutions for large enterprises in a variety of industries: airlines, travel companies, telecoms, financial institutions, as well as retail and consumer goods companies. Comarch's CRM & Marketing portfolio – which includes the award-winning Comarch Loyalty Management (CLM) system – is an advanced set of solutions dedicated to marketing processes and activities, building loyalty and maximizing engagement. Comarch is a true end-to-end loyalty and engagement provider. Aside from best-in class technology and product sets, Comarch also offers a full suite of managed services to guide customers throughout the entire loyalty program lifecycle. With thousands of successfully completed projects, 20 data center locations and more than 6,500 employees in over 90 offices around the world, Comarch has the support and infrastructure necessary for high-volume rollouts.

www.comarch.com | info@comarch.com