VOLUME 3, 2020

LSA

BEST PRACTICE GUIDE

ACCOUNT TAKEOVER

LSA
LOYALTY SECURITY ASSOCIATION

TABLE OF CONTENTS

03 Introduction

04 What is Account Takeover?

04 How Does Account Takeover Affect Loyalty Programs?

05 Points Mean Prizes. And More

05 But Why Now - What's Changed?

07 How Fraudsters Are Monetizing Loyalty Program Account Takeover

07 What the Fraud Flow of Loyalty Program Account Takeover Looks Like

08 The Consequences

- Losing Loyal Customers.....8
- Losing Valuable Customers.....9

10 Why Does Loyalty Program Account Takeover Go Undetected?

- Bad Security Protocols.....11
- Bad Bot Protection.....11
- Not Monitoring your Loyalty Program.....11
- No Transaction.....11
- Saved Payment Details.....12
- Loyalty Program Marked Low Risk.....12
- Less Awareness of Loyalty Fraud.....12

13 The Key to Detecting Loyalty Program Account Takeover is Visibility

14 Highlights

15 Contributor

LSA
LOYALTY SECURITY ASSOCIATION

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

Account Takeover

What is Account Takeover?

Account takeover (ATO) occurs when a fraudster gains unauthorized access to a customer account and monetizes that access by manipulating account information, making transactions, or stealing PII. Both manual & automated (bots and emulators) attack vectors, paired with advanced evasive techniques, are used to execute these attacks.

In this volume

- What is Account Takeover (ATO)
- How ATO fraud affects loyalty programs
- Why are ATO attacks on loyalty programs so difficult to detect?
- Steps to protect your program

How Does Account Takeover Affect Loyalty Programs?

ATO is a common method used to perpetuate rewards program fraud. These attacks affect **72%** of loyalty programs. Accessing these user accounts gives attackers access to saved payment details, additional PII, and other perks like account reputation. In addition to the common motivations for executing this type of attack, loyalty points sweeten the pot for fraudsters. Monetization is straightforward and quick as points are transferred into an account owned by the fraudster - all before any alerts of suspicious activity can be raised. Detection comes after the fact, and the damage is already done.

POINTS MEAN PRIZES. AND MORE

Rewards programs are popular with businesses and consumers, but these programs are a repository of three things criminals want:

POINTS	CUSTOMER DATA	CREDIT CARD
redeemable against goods and services	that can be used in further attacks	and other payment information

BUT WHY NOW - WHAT'S CHANGED?

For merchants, "loyalty can have two major business impacts: revenue and reach" and has therefore led to a revolution in the customer loyalty marketing: Continued investment in developing competitive, engaging rewards programs brought the global value of rewards accounts up to an estimated $250 billion mid-2019.

As merchants compete to attract and retain their loyal customers, the value and liquidity of the points continue to rise. Reward and loyalty points are essentially a form of currency. Points can be exchanged for cash, goods and can also be converted into cash-like gift cards. And the impact of loyalty fraud can be just as damaging a traditional payment fraud.

All this adds up to an extremely lucrative target for fraudsters. But that's not all.

BUT WHY NOW - WHAT'S CHANGED? - CONTINUED

Apart from being more valuable than ever, loyalty accounts are also the most vulnerable:

CREDENTIAL DUMPS & PASSWORD REUSE	SECURITY IS LACKING	AWARENESS IS LACKING
With the amount of stolen PII available on the dark web, the chances that fraudsters can beat (or even bypass) this security control, are exceptionally high.	When it comes to protecting loyalty programs, security is almost never a priority. A simple email and password combination or a 4-digit PIN, are still often considered sufficient. As a result, loyalty programs are low-hanging fruit for fraudsters.	Customers don't monitor their loyalty accounts as closely as they do their bank accounts or credit card statements. Some don't ever check them. As a result, loyalty program fraud can go undetected for months, if not forever.

HOW FRAUDSTERS ARE MONETIZING LOYALTY PROGRAM ACCOUNT TAKEOVER

WHAT THE FRAUD FLOW OF LOYALTY PROGRAM ACCOUNT TAKEOVER LOOKS LIKE

In order to best understand the fraud flow of the fraudster's journey, we can align the stages of the attack with that of the customer journey, the login, session and checkout. The following table represents common monetization tactics fraudsters can employ throughout their attack. Note how a significant portion can take place before they even arrive at the checkout stage.

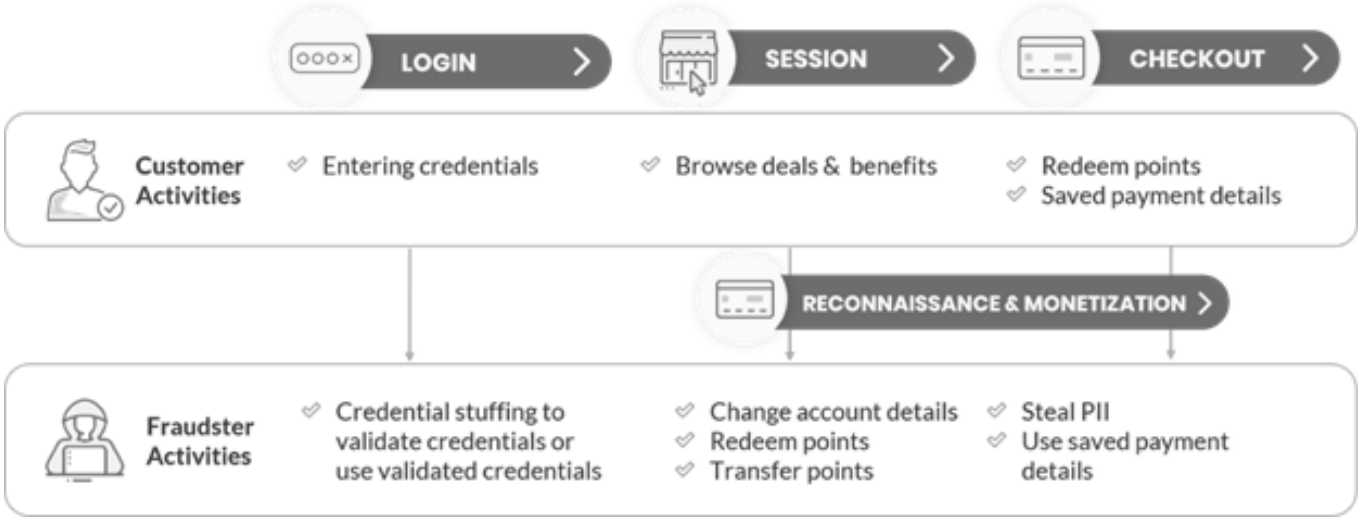

Image 1: The Fraudster's Journey of Loyalty Program Account Takeover

Further monetization can take place outside of the account based tactics, this can include selling PII or validated account credentials with points on the dark web or even re-selling goods or services on legitimate forums.

Losses from loyalty and reward points fraud add up to an estimated **$1 billion** annually. With **14 trillion frequent flier miles and hotel points valued** at **$140 billion in unspent loyalty points** floating around unused, it's clear that attacks on loyalty programs pose a serious threat.

THE CONSEQUENCES

The immediate consequence of loyalty program account takeover includes the direct loss of revenue in case fraudsters make a transaction. But ATO attacks on loyalty programs have a much wider and long-lasting impact than the immediate losses.

- Cause operational overhead due to the need to manually reset or investigate the account
- Can damage your reputation
- Expose the company to PII leakage liability

Losing Loyal Customers

What sets these attacks apart is that they target your most loyal customers. Loyalty program fraud jeopardizes your customers' confidence in your brand and can make it difficult to gain new customers. It is capable of derailing customer relationships and causing millions of dollars of damages and ruining company reputations.

- Two of three consumers who shop online said they would stop buying from retailers if their accounts were compromised
- More than half (54%) would delete their accounts altogether 39% of respondents would go to a competitor in the event of an account breach, and one in three would tell friends to stop shopping with a retailer.

Source

THE CONSEQUENCES - CONTINUED

Losing Valuable Customers

Companies heavily invest in their loyalty programs because returning customers are key to improving customer lifetime value (LTV) and increasing profitability - 71% of Companies Invest 2% of Total Revenue in Loyalty & CRM. McKinsey & Company states that US companies spend $50 billion a year on loyalty programs alone. If done rightly, loyalty programs can generate as much as 20 percent of a company's profits. Research shows that it costs a business up to 25 times more to acquire new customers than selling to an existing one.

WHAT'S THE CONNECTION BETWEEN LTV & FRAUD?

Why Does Loyalty Program Account Takeover Go Undetected?

Account Takeover is one of the most dangerous types of eCommerce fraud. Loyalty program theft can go undetected for months, if not altogether.

This happens to a large extent because fraud prevention programs are not calibrated to detect loyalty program fraud. Often fraud detection is tied to one particular stage or action in the customer journey, mostly at the payment stage. But ATO attacks are focused on monetizing much earlier than the payment stage, bypassing even the need to complete a traditional transaction.

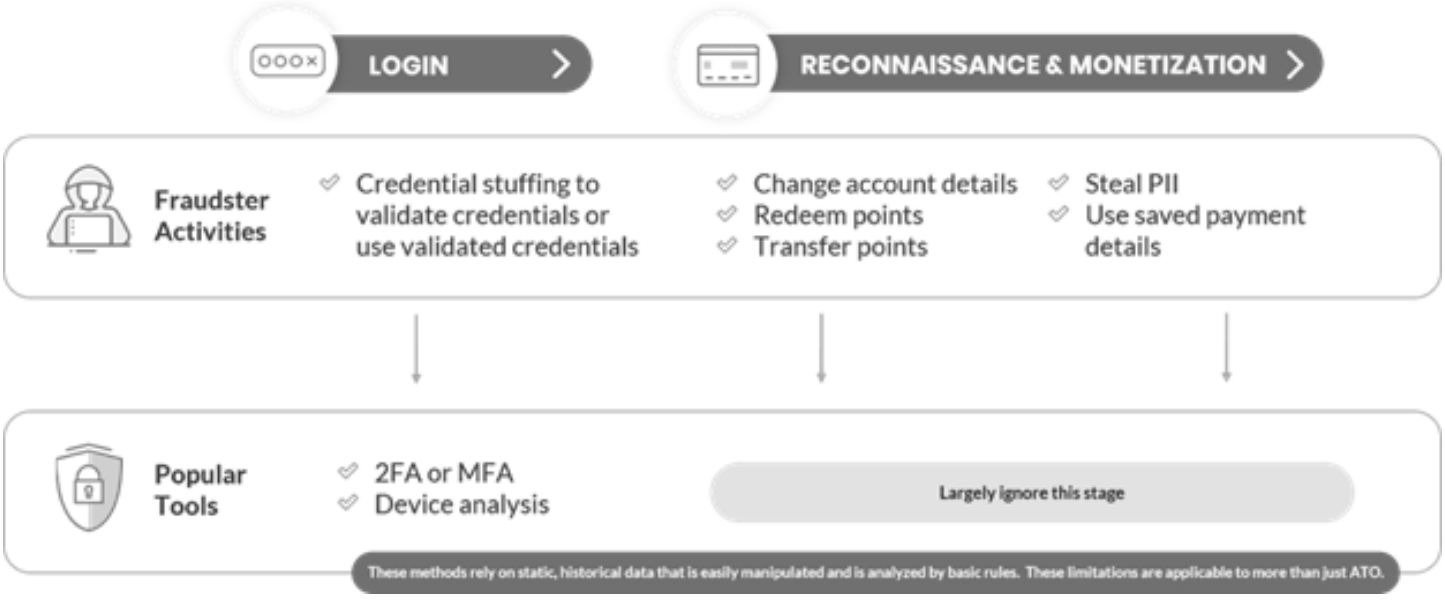

Image 2: The Fraudster's Journey of Loyalty Program Account Takeover vs Popular Fraud Detection Solutions

Why Does Loyalty Program Account Takeover Go Undetected? - continued

The fraudster's journey is not so simple as a quick login, transaction, and log out. They now look for other vulnerabilities to get the highest ROI they can: looking for other ways to monetize either by exchanging loyalty points for goods and cash, stealing PII, changing account settings, or occurring and transferring loyalty points.

- **Unsophisticated security controls.** Loyalty programs' security controls are mostly extremely basic, often just username & password - which are easily accessible on the dark web. The use of legitimate credentials is not going to raise any flags.
- **None or unsophisticated bot protection.** Loyalty programs are unlikely to have any kind of bot detection solution in place. Being able to identify credential stuffing bots, the first stage of an ATO attack, is critical.
- **You are not closely monitoring your reward program.** Monetization of a reward account can happen long before any type of transaction happens. Since most fraud programs are calibrated to monitor transactions, you can't see what you are not looking for.
- **No monetary transaction takes place.** The majority of transactions are not traditional transactions, they consist of redeeming or transferring points or stealing PII - both activities don't trigger most fraud alerts.

Why Does Loyalty Program Account Takeover Go Undetected? - continued

- **Using saved payment details.** Even if a transaction does take place, it's more than likely to use the saved legitimate- payment details so no reason for the transaction to be flagged or rejected.
- **Loyalty program accounts are often marked as low risk.** Frequent account usage and the variety of purchases associated with accounts means that account is known to the merchant and is considered "reputable". This account reputation has a direct effect on risk scores when unusual transactions are made, leading to false negatives and very high thresholds for fraud alerts.
- **Less awareness.** Finally, unlike the other types of fraud vectors, customers are less aware of this type of fraud. This lack of awareness makes it easy for fraudsters to stay under the radar. Since no monetary transaction takes place, merchants often are only alerted of fraud by their customers who find their hard-earned rewards gone from their accounts, often months or years after the fact.

Stolen and validated credentials are so easy to get a hold of and once a user is passed that stage, they can monetize the rewards program without having to pass through any other security until they get to the payment stage. Fraudsters can do enough damage to the rewards account without ever having to get to the checkout.

The Key to Detecting Loyalty Program Account Takeover is Visibility

Loyalty fraud involves attacks at multiple touchpoints throughout the customer journey from the log in process to the transaction and final redemption of points. In an era when customers expect rewards for their business, it's essential to make sure your loyalty program is safe and secure. **Ultimately, it means that loyalty program fraud protection requires oversight into the entire customer journey.**

Behavioral Biometrics is not tied to any one activity of the customer journey. From the moment a session begins, it continuously monitors user behavioral patterns throughout the customer journey. This means that suspicious behavior can be flagged before any type of transaction takes place and the damage is done.

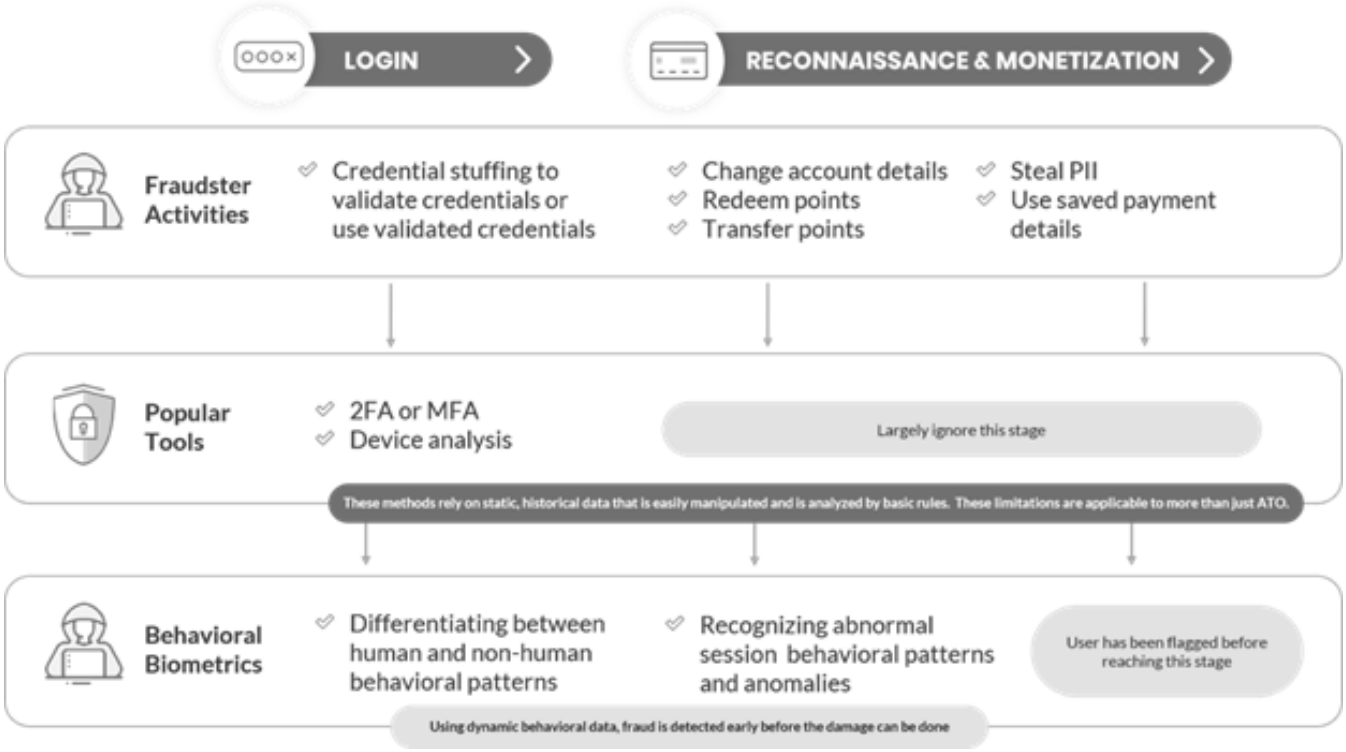

Image 3: The Fraudster's Journey of Loyalty Program Account Takeover vs Popular Fraud Detection Solutions vs Behavioral Biometrics

Highlights

- ATO attacks affect 72% of Loyalty Programs
- With Loyalty Fraud costing an estimated $1 Billion annually, businesses must find effective ways to protect their loyalty programs
- Loyalty fraud is especially difficult to detect since most fraud detection tools are calibrated to detect payment fraud
- Loyalty fraud involves attacks at multiple touchpoints throughout the customer journey from the login to the transaction and final redemption of points.
- Only by continuously monitoring buyer behavior throughout the customer journey can loyalty programs be truly protected from fraud.
- Behavioral biometrics provides visibility of the entire customer journey to detect fraud early before the damage is done

This volume was written by

SECUREDTOUCH

SecuredTouch is the expert in behavioral biometrics-based fraud detection solutions for online merchants and financial institutions. Using machine learning, the technology continuously analyzes hundreds of unique behavioral data points to differentiate between human and non-human behaviors, human to device interactions and behavioral anomalies to provide early detection of fraud before the damage is done. The solution identifies sophisticated fraud from the moment a session begins throughout the customer journey while simultaneously improving the user experience. Businesses benefit from reduced drain on internal resources and increased transaction rates, ultimately leading to an improved bottom line. Today, our award-winning solutions are used by some of the world's largest retailers and financial institutions.

www.securedtouch.com

Name:

Password:

LSA
LOYALTY SECURITY ASSOCIATION