NETACEA / WHITEPAPER

Customer Loyalty:
How are bots exploiting businesses?

NETACEA

INTRODUCTION TO LOYALTY FRAUD

Loyalty reward schemes have been a regular feature of the eCommerce landscape for the past two decades, with points accumulated based on repeated custom and faithful purchases. The more loyal the customer, the more rewards are available to redeem. Loyalty is rewarded in various ways; often the points gathered are redeemable against the primary business – like popular international supermarkets, airlines and hotel chains. Other schemes offer the flexibility to spend the points elsewhere, taking advantage of third-party services, products and experiences.

Unfortunately for businesses, loyalty programs are as attractive to cybercriminals as they are to customers. For years, adversaries have been exploiting loyalty schemes to access personally identifiable information (PII) and purchase products or services to use or resell for a healthy profit. Loyalty point memberships were expected to reach 5.5 billion worldwide by the end of 2020.[1] With reward schemes more appealing than ever, loyalty point fraud is becoming an increasingly sophisticated and growing problem for the eCommerce, airline and hospitality industries.

Sources:
[1] Travel Weekly: Latest targets of fraudsters are hotel and airline loyalty points

THE GROWTH OF LOYALTY SCHEMES IN 2020

The global eCommerce market saw unprecedented growth during the pandemic, with digital activity accelerated by the demand for online services, from grocery shopping to PPE supplies. Predicted to reach $5.4 trillion in 2022, the industry saw evolving consumer habits taking shape as a result of Covid-19, creating an urgency for brands to rethink their loyalty point offerings.[2] A recent McKinsey study revealed that more than 75% of consumers 'tried new brands, places to shop or methods of shopping during the pandemic', and that businesses launched, updated or expanded their loyalty programs to accommodate this change in behavior.[3]

Businesses have also used loyalty points as a way of bringing customers back to their brand after a turbulent economic year.

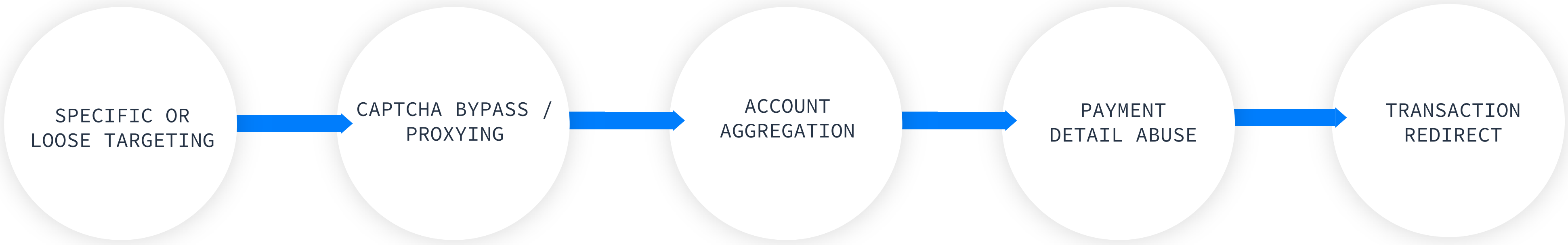
Paid loyalty programs offer an attractive option for businesses to both onboard new customers and to ensure long-term customer value at a time when the growth of eCommerce platforms and saturated omnichannel experience makes for a tough fight for customer loyalty. 62% of customers said they were more likely to spend more on the brand since joining their paid loyalty program, while 59% would choose the brand more over its competitors since signing up.[4] From credit vouchers for cancelled holidays to accrued loyalty points from repeated eCommerce purchases, an increase in shoppers opening various loyalty point accounts and accumulating a range of points across these accounts amounts to increased opportunity for cybercriminals to exploit reward schemes.

Sources:
[2] Stastista: Worldwide retail eCommerce sales
[3] Marketing Dive: What Covid-19 did to customer loyalty
[4] McKinsey: Coping with the big switch: How paid loyalty programs can help bring consumers back to your brand

UNDERSTANDING LOYALTY FRAUD THROUGH THE BLADE FRAMEWORK

Netacea's BLADE (Business Logic Attack Definition) framework captures the various stages of a loyalty fraud attack, from resource development, reconnaissance and defense bypass, through to attack preparation, execution and post-attack action.[5] Using this framework, businesses can isolate the individual attack stages used by the adversary to gain access to loyalty point accounts, allowing for improved risk assessment, strengthened threat detection and mitigation capabilities, and a better-informed incident response process.

Loyalty fraud attacks usually begin with the attacker obtaining username and passwords from the dark web or even a public-facing forum and using credential stuffing to inject these credentials into various websites with known loyalty programs until they get a match. Techniques such as proxying and CAPTCHA bypass are used to circumvent defense mechanisms, and account aggregation techniques are used to consolidate information and gain access to multiple accounts in order to move loyalty points around. We then see misleading payment details being fed into checkout pages, after which the smartest thing attackers can do is to quickly move those accrued points elsewhere where there is no trail of the targeted business, and the credit becomes out of its control.


SPECIFIC OR LOOSE TARGETING

CAPTCHA BYPASS / PROXYING

ACCOUNT AGGREGATION

PAYMENT DETAIL ABUSE

TRANSACTION REDIRECT

Sources:
[5] BLADE Framework

TARGETING THE TRAVEL AND ECOMMERCE INDUSTRIES WITH LOYALTY POINT ABUSE

Loyalty points are stolen and sold on the dark web for a fraction of the price they are worth. Adversaries either cash out the stolen loyalty points to sell on for a profit or transfer them to another account to exploit a third party. The last year has seen some high-profile attacks on travel loyalty schemes, including global hotel chain Marriott, which in 2020 suffered a security breach on hotel guests who used the company's loyalty app, impacting more than five million customers.[6]

Frequent flyer miles are also popular among these types of attackers. 55% of consumers still enjoy earning travel rewards through their loyalty program or credit card, many with plans to redeem these for travel-related benefits as soon as possible.[7] A batch of flyer miles can be purchased on the dark web for as little as $31 dollars, and 200,000 airline points (worth approx. $2000) can sell on the dark web for just $45.

As the loyalty industry grows, businesses must stay alert to avoid the threat of adversaries. Due to the fact 45% of loyalty point accounts are inactive, many are vulnerable to attack.[8] It's predicted that annual loyalty point fraud will soon surpass traditional credit card fraud – which currently amounts to between $4 billion and $5 billion annually – meaning it is more important than ever for businesses to treat loyalty point abuse with the same seriousness as monetary fraud.[9]

Why will loyalty fraud overtake credit card fraud?

- Loyalty point fraud is much harder to track than monetary transactions. Accounts are checked by customers far less frequently than bank accounts, and customers generally do not keep a close eye on account valuables.
- Businesses often neglect point accounts and prioritise 'legitimate' currency attacks like credit card abuse.
- Loyalty points are often easily used or transferable either within the targeted company or via a third-party service.

Sources:

[6] ZDNet: The biggest hacks, data breaches of 2020

[7] Auriemma Group: COVID-19's Impact on Travel Has Shifted Consumer Loyalty Needs

[8] Travel Weekly: Latest targets of fraudsters are hotel and airline loyalty points

[9] Travel Weekly: Latest targets of fraudsters are hotel and airline loyalty points

How does loyalty fraud cost businesses?

Aside from the reputational repercussions associated with suffering a breach of customer credentials, the financial cost of loyalty point fraud to businesses can be categorised threefold:

1. Losing the original value of the loyalty points / credit to the adversary.
2. Reimbursing the affected customers with the monetary value or loyalty credit stolen in the attack.
3. Losing the currency out of the business' ecosystem. According to Auriemma's latest research, 76% of credit cardholders enrolled in a loyalty scheme prefer to use their loyalty rewards for non-travel benefits. While adversaries can redeem the points or credit against the targeted company, through avenues like supermarket point schemes they are able to spend the value of the points in other shops or on other services.[10]

As more customer accounts are created, the attack surface for loyalty point fraudsters increases, as does the opportunity for them to exploit multiple accounts. Netacea has witnessed a rise in account aggregation as customers create more loyalty accounts across various websites and reuse passwords across various accounts. Passwords are regularly available across both the open and dark web – some you don't even have to pay for – as we have moved into a world where credentials are available on public-facing services. Thousands of credentials are flooding the web every day, even via social media, and a quick Google search will find you thousands of breached usernames and passwords. Password reuse creates a low barrier to entry for attackers who take advantage of poor security and attack multiple accounts using the same username and password credentials. Unfortunately for businesses, they are only as secure as their customer's weakest password and account. This means attackers can use credentials to breach a lower-security small website, then if successful use those same credentials to target a larger entity.

Sources:
[10] Auriemma Group: COVID-19's Impact on Travel Has Shifted Consumer Loyalty Needs

TOOLS USED BY ADVERSARIES TO EXECUTE LOYALTY FRAUD

Adversaries are becoming far more advanced with the tools they use to execute loyalty point fraud. We have moved to a world where credentials are readily available online, even on public-facing forums and social media, making credential stuffing ever easier for attackers.

Netacea protects a global fast-food chain against the threat of loyalty point fraud which was targeting the business. One particular investigation discovered user login credentials on publicly available online forums and marketplaces, and adversaries abusing customer accounts across the globe using these stolen credentials. The theft of products through illicit orders using loyalty points meant both product and financial loss for the company.

The tools extracted PII from compromised customer accounts, presenting a data protection issue and increasing the risk of future attacks as credentials are reused across the internet by adversary groups. On the worst days, 90% of account logins came from attackers. These sophisticated tools developed by the attackers allowed them to purchase goods for free or at a lower cost, and abuse bonus awards such as loyalty points.

Sentry MBA is the most popular and widely used credential stuffing tool, and the most recognizable in credential stuffing attacks and loyalty point fraud. Like most tools of its type, it has a user interface that allows the uploading of base credential lists and proxies, and a screen where results are logged. However, the newly emerged OpenBullet tool is a testing suite of software allowing users to perform requests on a target web application and has been gaining interest with cybercriminals since April 2019.[11]

> On the worst days, 90% of account logins came from attackers.

Sources:
[11] Digital Shadows: The rise of OpenBullet: A deep dive in the attacker's ATO toolkit

Further tools developed by adversaries to execute credential stuffing and subsequent loyalty point fraud:

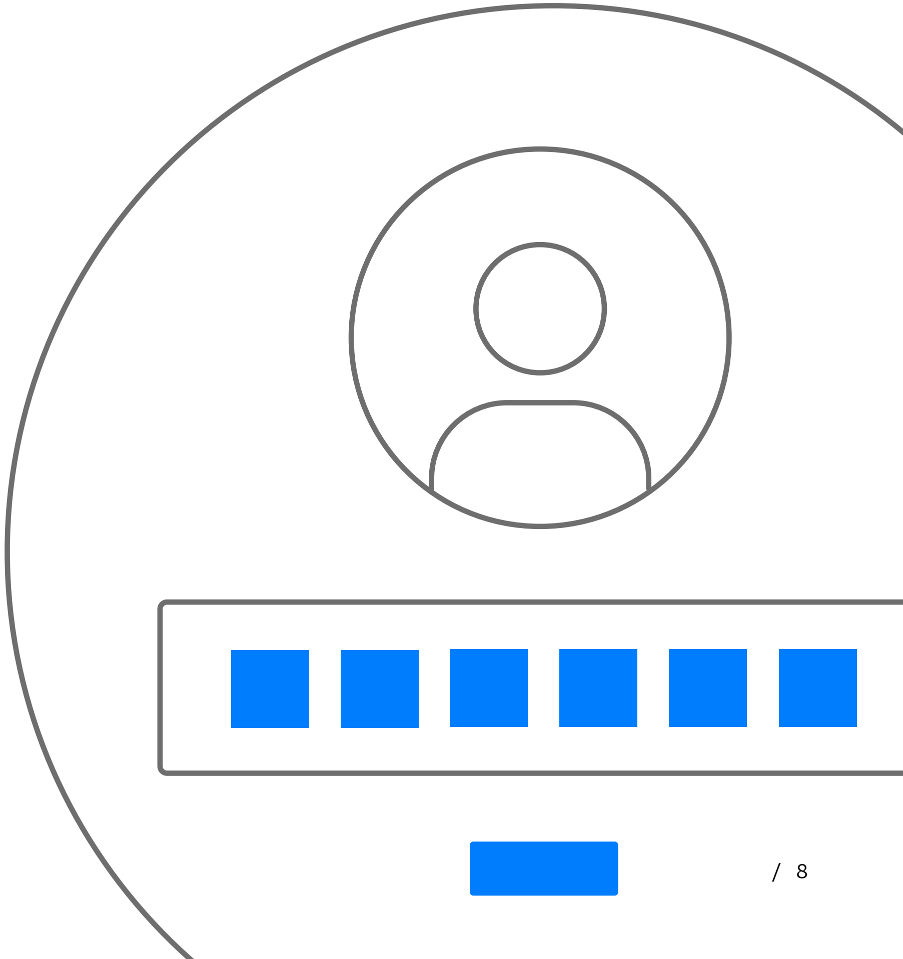
- **Vertex** requires users to supply a list of credentials and proxy servers, similar to Sentry MBA though not as popular and using different functionality. The software is still regularly used and advertised on carding and cracking sites.

- **SNIPR** has been around since April 2017, functioning similarly to Sentry MBA. It's installed with a variety of pre-built configurations for popular sites, including requested URLs, user agent strings, data capturing form requests, and the correct order of authentication, alongside an in-built mechanism for public proxy scraping or the ability to import specified lists.

- **Private Keeper** is a tool used across Russian language cybercriminal platforms. It contains a utility for collecting private proxies from other private services and provides access to multiple finished projects in an application store. Online tutorials explain how to use Private Keeper for specific targets such as financial organizations.

- **Account Hitman** is not specifically a credential validation tool, but the software requires credential lists and proxy server lists to attack website login portals, similar to Sentry MBA and Vertex. Appealing to less technically advanced users, Account Hitman is a predictable choice for novice threat actors.

- **BlackBullet** is an increasingly popular tool. A BlackBullet user is required to list username and password combinations to try on a web application and a list of proxy servers. This counters businesses' attempts to deter credential stuffing with IP address limitations.



EXPANDING THE ATTACK LANDSCAPE

As customers create more accounts across various sites and reuse passwords, the opportunity for adversaries to attack multiple accounts with the same credentials also grows. There are hundreds of e-wallets and apps available online which allow customers to aggregate their loyalty accounts into one tidy depository, but a lack of password security creates a low barrier to entry for attackers, who, once they have obtained a set of credentials, have access to multiple customer loyalty accounts to abuse across sites.

Netacea investigated the use of such apps and e-wallets and found that adversaries were taking advantage of this low barrier to entry on a particular app to redeem customer loyalty points at a global supermarket.

The challenge
The mobile wallet is built for storing various loyalty points from different accounts. It is free to download and sign up to on any application. Customers store virtual loyalty point cards which work the same as physical loyalty cards by adding in unique bar codes. The lack of two-factor authentication makes for an insecure password system, meaning a low barrier to entry for attackers.

The outcome
Netacea discovered a mixture of open-source information being sold online including customer credentials for a large supermarket chain. Our Threat Research team explored how adversaries use e-wallets to exploit secondary companies and discovered that adversaries were breaching virtual supermarket accounts by adding the barcode for each account into the e-wallet, then buying supermarket goods with somebody else's loyalty points.

PROTECTING YOUR BUSINESS AND CUSTOMERS AGAINST LOYALTY

Responsibility for preventing loyalty point fraud lies with both the customer and the business. It's crucial that customers use different passwords for accounts across the internet, use a password manager to keep track of this, and ensure they are monitoring their loyalty accounts to make sure they know what their balance is, what's been redeemed and if there's been suspicious activity.

While every business would hope that its customers take their own security seriously to help reduce this type of fraud, it's vital businesses make logging into customer accounts as secure as possible to raise the barrier to entry for adversaries trying to gain access. Businesses must treat loyalty points with the same level of stringency as 'legitimate' currency and not rely on strong customer password use to stop attackers. Any that view this type of fraud as secondary to card fraud are at risk of remaining on the back foot against attackers.

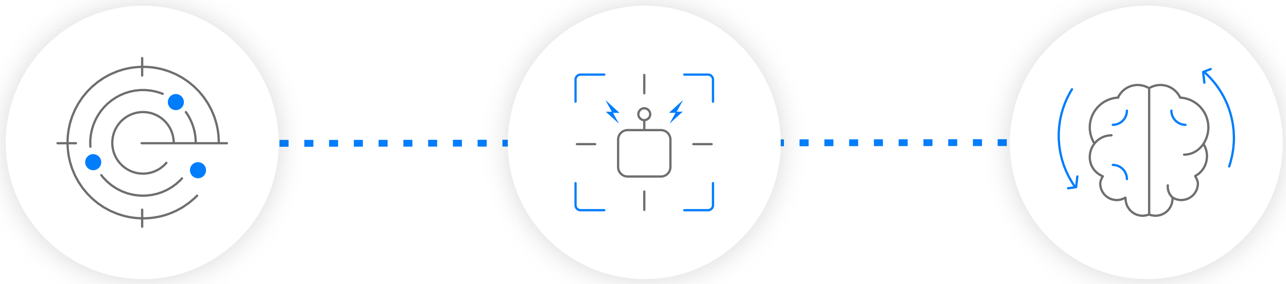
Top tips for protecting your business against loyalty fraud include:

- Implement multi-factor authentication (MFA) on login pages to alert customers to suspicious login activity on loyalty accounts.
- Secure third-party systems, e-wallets and plugins to decrease the surface area available to adversaries.
- Monitor traffic across loyalty point schemes; ensure you have an overview of who is using them and whether the traffic is from malicious bots or human users.
- Use CAPTCHA.
- Separate username and password fields with a two-step process.

USING ADVANCED BOT MANAGEMENT

Netacea Bot Management protects your websites, mobile apps and APIs from loyalty point fraud. Our Intent Analytics™ Engine uses advanced machine learning techniques to detect loyalty fraud attempts by spotting patterns of logins that indicate suspicious behavior.

- Real-time analysis powered by Intent Analytics™
- Best-of-breed anomaly detection
- Threat intelligence feed
- Insightful, data-rich dashboards
- Total control over response options
- Seamless and flexible integrations
- Dedicated bot experts with 24/7 support



DETECT MALICIOUS BOTS

RESPOND TO ATTACKS

EVOLVE AND ADAPT

Sign up for a free trial to see how Netacea can detect and stop sophisticated automated threats such as loyalty points abuse for your business.