Points of Attack: Uncovering Cyber Threats and Fraud in Loyalty Systems

The better the question.
The better the answer.
The better the world works.

EY

Shape the future with confidence

Contents

Executive Summary

Executive Summary

Loyalty programs, once regarded as straightforward marketing initiatives, have transformed into complex digital ecosystems that represent billions of dollars in stored value. These systems enable businesses to track customer behavior, reward loyalty, and personalize experiences, but they also introduce a critical cybersecurity blind spot. With the convergence of mobile apps, APIs, backend databases, and third-party vendors, loyalty systems now mirror many of the same structural complexities — and vulnerabilities — of digital financial platforms, yet without equivalent security maturity.

Cybercriminals have taken notice. The global value of loyalty points is estimated to exceed $200 billion, with 30–50% of these points going unused — making them a prime target for exploitation. Loyalty accounts are increasingly being treated as soft digital wallets, targeted through credential stuffing, API exploitation, automated fraud bots, and phishing campaigns. Attackers use tools like OpenBullet, Snipr, and residential proxies to bypass fraud detection, harvest reward points, or manipulate redemptions.

Notably, these attacks often go undetected for months. The average time to detect loyalty fraud ranges from 150 to 180 days, allowing for sustained and repeated abuse. Furthermore, loyalty points are actively traded on the dark web, typically at 10–20% of their retail value, providing an anonymous and scalable method of monetization.

This advisory explores the modern threat landscape surrounding retail loyalty programs, analyzing the motivations, tools, and methods used by attackers. It presents real-world case studies of loyalty fraud across airlines, e-commerce, and grocery retail sectors — demonstrating both technical and business logic vulnerabilities.

In addition to dissecting attack techniques, this report outlines effective mitigation strategies, including:

- Real-time monitoring and behavioral analytics.
- API security best practices and OpenAPI testing.
- Business logic testing and red teaming.
- Insider threat detection.
- Adoption of Zero Trust principles for loyalty ecosystems.

With AI-powered fraud, synthetic identity creation, and reverse-engineering of mobile loyalty apps on the rise, it is imperative that retailers and cybersecurity teams elevate loyalty system security to the same critical tier as payment infrastructure. Strategic recommendations and a five-level maturity model are presented to guide organizations on their path to resilience.

Purpose and Scope:

This advisory report provides a detailed examination of the evolving cybersecurity risks and fraud mechanisms affecting retail loyalty program ecosystems. While traditional threat assessments often prioritize core IT systems, payment infrastructure, or customer-facing applications, loyalty platforms remain an under protected domains despite their increasing importance in digital commerce.

CISOs and security architects, responsible for system resilience.

Threat intelligence analysts, tracking adversary infrastructure.

This analysis is relevant to a cross-functional audience, including:

Fraud and risk management teams, monitoring loyalty abuse.

Business and loyalty program managers, overseeing customer engagement platforms.

By focusing on the intersection of technology, business logic, and user behavior, this report highlights why loyalty systems must be treated as critical infrastructure and secured accordingly.

Security Risks in Loyalty Programs

Valuable Targets with Real-World Worth: Loyalty points often hold monetary value, are transferable, or convertible to goods and cash — making them attractive theft targets.

Credential Reuse and Poor User Hygiene: Reused passwords and breached credentials make loyalty accounts easy targets for credential stuffing and account takeover.

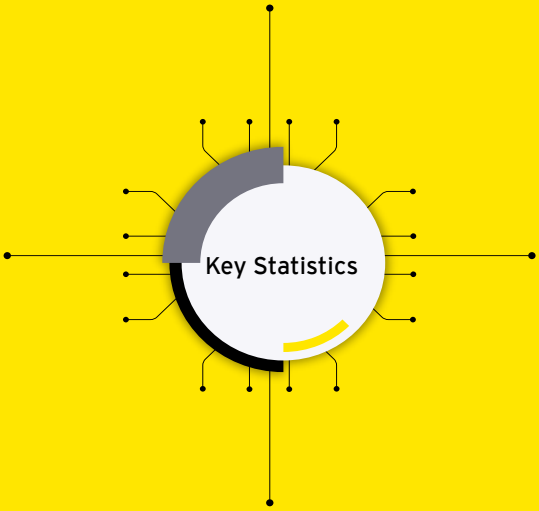
Low Monitoring and Organizational Priority: Loyalty fraud often goes undetected due to weak monitoring, delayed responses, and its treatment as a marketing — not a security — function.

Exploitable Business Logic and Workflows: Attackers abuse flaws like earning points from canceled orders, exploiting referrals, or manipulating tier upgrades.

Weak Security Compared to Financial Platforms: Loyalty systems typically lack strong defenses like MFA, device fingerprinting, or fraud analytics found in banking apps

89% increase in loyalty fraud since 2019.

75% increase in users manipulating store reward programs for fraudulent gain was reported by Merchant Fraud Journal in 2022.



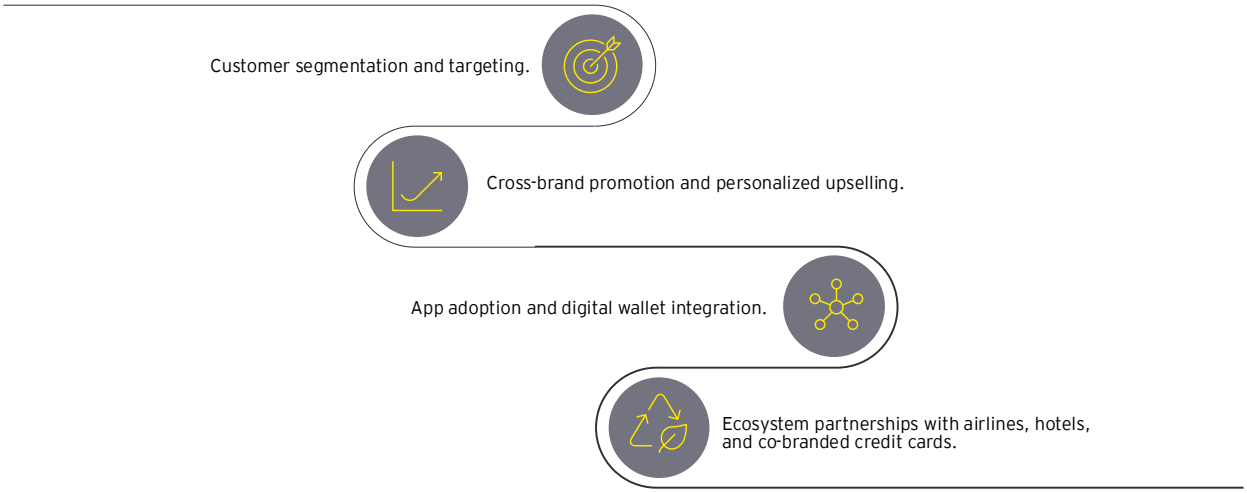
72% of customer loyalty programs have reported some type of theft or fraud, reported by Paystone in 2019.

$3.1 billion of redeemed loyalty points were fraudulent in the U.S., reported by Loyalty Security Association (LSA) in 2020.

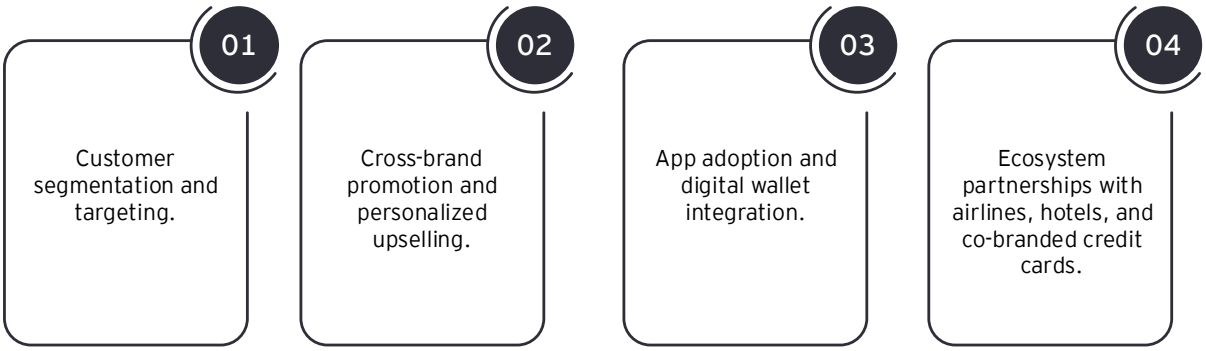
16.6 loyalty programs on average are owned by a U.S. consumer, according to Statista in 2022. However, only a small portion of the accounts are active, which leave the remainders the prime target for account takeover by fraudsters.

The Strategic Role of Loyalty Programs in Retail

Loyalty programs have become fundamental to customer retention and competitive differentiation in the retail sector. No longer peripheral marketing tools, these platforms now serve as data-driven engines powering:



Option



In mature retail environments, loyalty data feeds into product recommendation engines, pricing models, and revenue forecasts, thereby influencing top-line growth. For global retailers, loyalty platforms often operate at a scale similar to core banking systems — with millions of users, billions of data points, and real-time transactional flows.

However, this increased reliance also introduces systemic risk. As loyalty platforms grow in complexity and integration depth, they become attractive and viable attack surfaces for financially motivated adversaries.

Writing Credits

Anastasia Lou Regen, CISSP

Partner, Technology Consulting, Cybersecurity, EY Canada

Umang Handa

Partner at EY, Cybersecurity, EY Canada

Nick Galletto

National Cybersecurity, Strategy, Risk, Compliance and Resilience Leader, EY Canada

Loyalty economy market and threat landscape

Loyalty economy market and threat landscape

The global loyalty economy has witnessed a remarkable evolution over the past decade. Once considered supplemental to retail operations, loyalty programs have emerged as core business drivers, enabling targeted promotions, repeat purchases, and data-driven insights into consumer behavior. However, as their financial and operational significance has grown, so too has their exposure to fraud and cyber threats.

This section examines the scale, economic value, and emerging threat patterns associated with loyalty ecosystems, particularly in retail environments.

Global Value of Loyalty Points	As of 2025, industry estimates place the total global value of unredeemed loyalty points in circulation at over $200 billion USD. This includes: ▪ Airline frequent flyer miles ▪ Hotel rewards ▪ Credit card cashback and points ▪ Retail and grocery loyalty balances ▪ App-based referral or tiered point systems The average consumer in developed markets is enrolled in 6–10 loyalty programs, yet engagement remains low. According to Bond Brand Loyalty and McKinsey, up to 30–50% of loyalty points are never redeemed, resulting in a vast reservoir of stagnant, under-monitored value. This latent value pool creates an environment similar to unused gift cards or dormant digital wallets — lucrative, minimally protected, and often overlooked until abuse occurs.
Loyalty Programs as Digital Wallets	The financialization of loyalty systems has prompted cybercriminals to treat them as **secondary wallets**. Points can now be: ▪ Exchanged for high-value products (e.g., electronics, vouchers). ▪ Traded on dark web marketplaces at a fraction of their retail value. ▪ Monetized via fraudulent resell or refund schemes. ▪ Aggregated using bots for mass redemption or laundering. Darknet analysis shows loyalty points being sold for 10–20% of their nominal value, with listings for: ▪ Airline miles (e.g., 100,000 miles for $800). ▪ Grocery store points with attached login credentials. ▪ Retail accounts offering "verified" access to loyalty balances. ▪ API tokens and authentication cookies for program access. In several underground forums, loyalty fraud is considered a low-risk, high-reward crime, as it avoids the more aggressively monitored payment rails and banking systems. This shifts the threat model from traditional finance-focused fraud to retail and loyalty system abuse.

Rise in Loyalty Fraud and Abuse

89% Year-Over-Year Increase in Loyalty Fraud: According to Forter's 2019 Fraud Attack Index, fraud attacks on loyalty programs surged by 89% between 2018 and 2019.

$1 Billion in Fraudulent Loyalty Redemptions Annually: Forter estimates approximately $1 billion in loyalty points are redeemed fraudulently each year in the U.S.

72% of Merchants Report Loyalty Program Fraud: Forter's NRF 2020 summary indicates 72% of loyalty program operators have experienced some form of fraud or abuse connected with their offerings.

Accounts Holding Loyalty Points Are 4–5× More Likely to Be Targeted: Forter's Trust Premium Report (2024) notes that accounts with loyalty balances are 4–5 times more likely to be attacked, especially among Gen Z and Millennial

Industry Specific Patterns

Different retail sectors experience unique loyalty fraud dynamics:

- **Airlines and Travel:** Frequent flyer miles are highly liquid and transferable, often targeted via credential stuffing or API-based enumeration of balances. Redemption fraud via travel bookings is common.
- **Grocery and Retail Chains:** Loyalty apps tied to phone numbers or barcodes are exploited via point-harvesting bots and insider abuse at checkout points. Cart abandonment and referral reward logic are often manipulated.
- **Luxury and Fashion:** High point-to-dollar ratios make loyalty accounts attractive for theft. Fake returns and tiered status abuse (e.g., VIP tier farming) are increasingly prevalent.
- **Pharmacy and Health Retail:** Loyalty programs linked to prescriptions or health data are abused through social engineering and fake account creation for reward farming.

Notable Breaches

Large UK Airlines (2022)	Largest hotel chain's loyalty program (2020–2022)	Canadian retail pharmacy chain (2023)	Large retail chain in UK (2024)
Attack Type: Credential stuffing.	**Attack Type:** API abuse & account enumeration.	**Attack Type:** Insider fraud.	**Attack Type:** Insider fraud
Impact: Tens of thousands of frequent flyer accounts compromised.	Impact: Millions of loyalty account records exposed	Impact: $500,000 in fraudulent redemptions.	Impact: Thousands of fraudulent point redemptions
Notes: Attackers used previously breached credentials; points were used for hotel and airline redemptions before detection.	**Notes:** Lack of rate limiting and poor token management enabled widespread data extraction.	**Notes:** Loyalty program staff issued duplicate redemptions and manually adjusted balances.	**Notes:** Attackers used rooted devices and app emulators to bypass redemption checks.

A Shifting Threat Surface

In the past, loyalty fraud was largely manual — requiring insider access, collusion, or basic phishing tactics. Today, adversaries deploy:

- Botnets and proxies to automate point harvesting.
- Mobile reverse engineering to bypass app validation.
- Custom scripts and fuzzers to abuse APIs.
- Machine learning models to mimic human redemption patterns.
- Deepfake voice phishing to impersonate customer service requests.

This signals a shift in threat landscape from opportunistic fraud to coordinated, scalable exploitation of loyalty infrastructure — often involving organized cybercriminal groups with monetization strategies that span multiple platforms and regions.

Types of Attacks Targeting Loyalty Programs

Types of Attacks Targeting Loyalty Programs

Loyalty platforms are increasingly targeted through a wide range of technical exploits, business logic abuse, and social engineering schemes. These attacks often span multiple layers — from mobile frontends and backend APIs to user behavior and operational workflows — allowing adversaries to harvest points, commit fraud, or gain unauthorized access to sensitive customer data. This section explores the primary attack vectors and abuse scenarios observed in real-world campaigns and threat research.

Account Takeover (ATO)

Account Takeover is the most prevalent attack method used to target loyalty platforms. ATO occurs when attackers gain unauthorized access to legitimate user accounts and perform fraudulent activities such as redeeming points, transferring rewards, or altering user credentials.

Common Techniques:

- **Credential Stuffing:** Automated testing of breached credentials (usernames and passwords) from other sites against loyalty login endpoints.
- **Password Spraying:** Using a few common passwords across many accounts to bypass lockout protections.
- **Phishing:** Emails or fake login portals mimicking loyalty brands to steal user credentials.
- **SIM Swapping:** Social engineering telcos to hijack a user's mobile number and intercept OTPs or recovery links.

Impact:

- Unauthorized redemption of points.
- Fraudulent bookings or purchases.
- Personal data exposure (e.g., travel history, contact info).
- Support overload from affected customers.

Case Example: A major airline loyalty program experienced a spike in password resets and unauthorized redemptions. Investigation revealed that attackers were using leaked credentials from a social forum, combined with IP rotation via residential proxies to bypass rate-limiting.

Theft and Redemption Fraud

Once access to an account is gained — or a vulnerability in point calculation is discovered — attackers aim to harvest and redeem loyalty points for personal gain or resale.

Methods of Theft:

- Automated point harvesting using bots to scan for low-security accounts.
- Bulk redemption of points for digital vouchers, gift cards, or services.
- Fake transactions to earn unearned points (e.g., abandoned carts, test purchases).
- Refund abuse to keep items and reclaim loyalty points simultaneously.

Common Redemption Fraud Tactics:

- Creating fake orders, canceling them after earning points.
- Exploiting loopholes in point expiration policies.
- Using multiple accounts for self-referral exploitation.

Business Risks:

- Financial loss due to unearned point redemption.
- Erosion of trust among legitimate customers.
- Manipulation of tier/status benefits.
- Increased fraud cost per transaction.

API Abuse

APIs are central to loyalty ecosystems — enabling mobile apps, partner platforms, and web services to interact with loyalty databases. Unfortunately, poor API hygiene is one of the most exploited technical vulnerabilities in loyalty fraud today.

Common Exploits:

- **Authentication Bypass**: Using tokens from one session to access another user's rewards.
- **Parameter Tampering**: Manipulating JSON payloads to modify point balances or redemption types.
- **Replay Attacks**: Reusing valid requests (e.g., point redemption) multiple times due to missing nonce or timestamp checks.
- **Fuzzing Endpoints**: Probing undocumented or partially documented APIs for logic flaws.

Real-World Vulnerabilities:

- Missing rate limits on point balance lookups.
- Unvalidated loyalty ID or phone number as sole identifier.
- Insecure direct object references (IDOR).

Case Insight: In a 2024 retail case, hackers fuzzed an internal loyalty redemption API and discovered that changing a single flag parameter allowed "premium gift" redemptions to go through without proper point deduction.

Business Logic Exploits

Unlike traditional technical exploits, business logic attacks exploit legitimate platform rules in unintended ways — often bypassing fraud detection entirely.

Common Patterns:

- **Cart Abandonment Abuse**: Earning points on orders that are later canceled or never completed.
- **Referral System Loops**: Creating multiple accounts to self-refer and earn stacking bonuses.
- **Tier Upgrade Abuse**: Exploiting tier triggers (e.g., spend thresholds) using fake purchases or refunds.
- **Double Redemption Bugs**: Submitting simultaneous requests for the same reward across channels.

These attacks are difficult to detect using standard technical monitoring because the requests appear valid, even though the behavior is abusive.

Organizational Risks:

- Financial leakage over time.
- Loyalty inflation and devaluation of tiers.
- Customer churn due to system manipulation.
- Complex detection and attribution.

Insider Threats

Not all attacks come from outside. Loyalty program fraud is increasingly tied to internal abuse by employees with privileged access.

Common Insider Scenarios:

- Manual point adjustment in customer accounts.
- Creation of fake accounts to earn fraudulent bonuses.
- Approval of non-qualified redemptions.
- Collusion with external actors for profit-sharing schemes.

Motives:

- Financial gain
- Targeted retaliation
- Exploiting inadequate internal controls

Example:

In a pharmacy chain, a loyalty program coordinator used internal tools to credit unearned points to dormant accounts, which were then monetized via gift card redemptions — costing the firm over $200,000 before being discovered during an audit.

Mobile App Reverse Engineering

Mobile apps often store or expose sensitive logic related to loyalty workflows — and attackers use reverse engineering tools to extract secrets, bypass security controls, or automate abuse.

Techniques:

- Decompiling APKs/IPA files to review loyalty program code.
- Intercepting API calls using tools like Burp Suite or Frida.
- Extracting hardcoded secrets (e.g., API keys, endpoint URLs).
- Bypassing client-side validations (e.g., reward eligibility).

Mobile emulators are also used for scripted farming of loyalty rewards, such as daily login bonuses or gamified earning schemes.

Risks:

- Token leakage
- Logic inversion
- App spoofing or impersonation

Phishing & Social Engineering

Attackers frequently impersonate loyalty brands via email, SMS, or social media to harvest user credentials, points, or personal data.

Tactics:

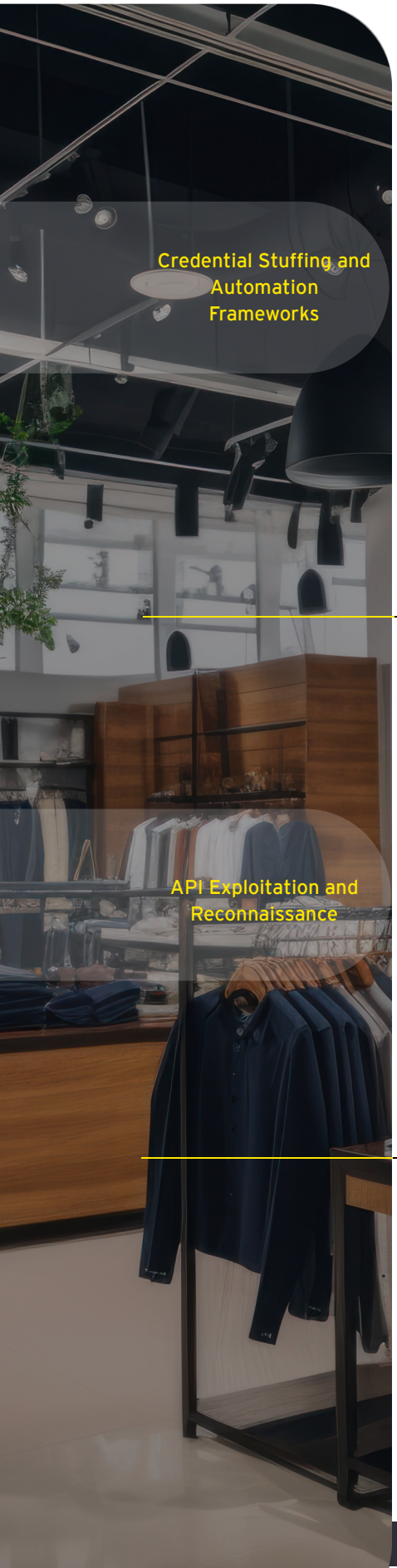
- Fake loyalty login pages mimicking well-known retailers.
- Promotional reward scams ("Claim 5,000 points now").
- Brand impersonation on social media to offer fake support or redemption portals.
- Deepfake voice fraud via customer support lines.

AI tools are increasingly used to:

- Personalize phishing templates using user data.
- Automatically generate loyalty-themed scam websites.
- Bypass CAPTCHA via OCR models.

Techniques and Tools Used by Attackers

Techniques and Tools Used by Attackers



Credential Stuffing and Automation Frameworks

Credential stuffing remains one of the most prolific techniques used to compromise loyalty accounts. Attackers leverage vast databases of leaked or purchased credentials — often from unrelated breaches — and test them against loyalty login endpoints at scale.

Tools Used:

- **OpenBullet**: A customizable credential stuffing framework that allows users to build "configs" for loyalty login portals. These configs enable automated testing of username/password combinations, handling of token-based logins, and session verification.
- **Snipr**: Similar to OpenBullet but with a more user-friendly interface, often used by novice cybercriminals.
- **SentryMBA**: A legacy tool that is still effective for brute-force attacks and has a large configuration marketplace.
- **BlackBullet**: An advanced tool that supports JavaScript parsing and dynamic flow handling for more secure portals.

Infrastructure:

- **Residential Proxies** (e.g., Luminati, Smartproxy): Used to bypass rate-limiting and geolocation checks.
- **CAPTCHA Solving Services**: Integration with services like 2Captcha or CapMonster allows attackers to bypass visual challenge-response mechanisms.
- **Combo Lists**: Username/password datasets sorted by geography, industry, or platform (e.g., "US Retail Loyalty Combos").

API Exploitation and Reconnaissance

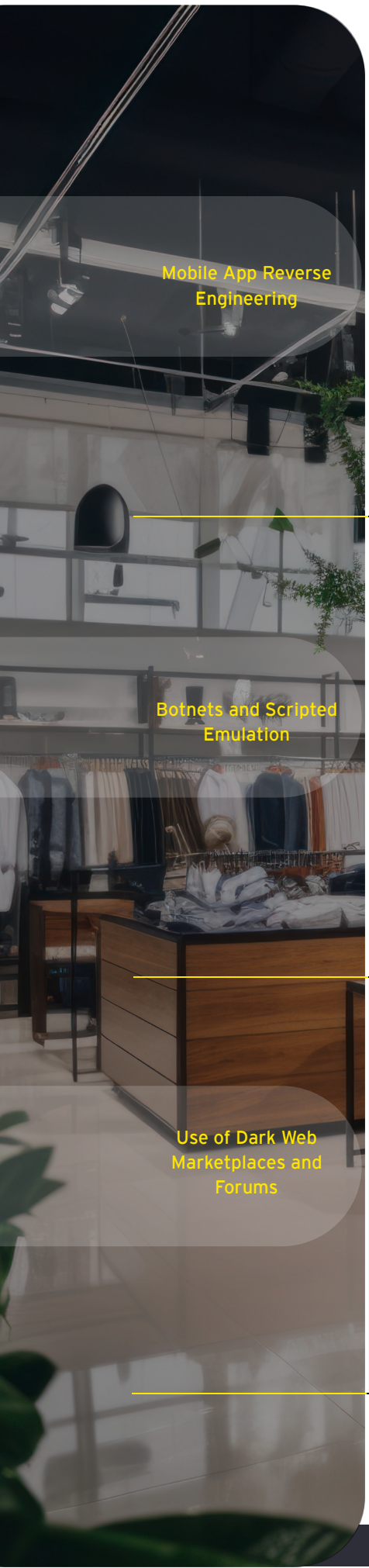
APIs are the lifeblood of loyalty programs, powering mobile apps, customer portals, and partner integrations. Attackers exploit insecure APIs using a combination of reconnaissance, testing tools, and replay automation.

Common Techniques:

- **API Enumeration**: Systematic testing of API endpoints for accessible functionality (e.g., GET /balance, POST /redeem).
- **Parameter Manipulation**: Altering values like user_id, tier, or points to observe system behavior or trigger unintended outcomes.
- **Replay Attacks**: Capturing and reusing valid requests to repeatedly redeem points or trigger rewards.
- **Token Reuse**: Using intercepted tokens from one session to impersonate another user due to missing session scoping or improper token validation.

Tools Used:

- **Burp Suite / OWASP ZAP**: Intercepting proxies used to inspect, replay, and fuzz API traffic.
- **Postman / Insomnia**: Often used during manual exploitation of known API endpoints.
- **Fiddler**: For Windows-based testing and session inspection of loyalty app traffic.



Mobile App Reverse Engineering

Attackers reverse-engineer loyalty mobile apps to extract logic, tokens, endpoints, and validation mechanisms.

Objectives:

- **Extracting Hardcoded Secrets**: Including API keys, encryption tokens, or secret URLs.
- **Understanding Business Logic**: Determining how points are calculated or redemptions are validated.
- **Bypassing Local Checks**: Such as in-app reward eligibility or tier validations.

Tools Used:

- **APKTool**: For decompiling Android APKs and accessing app resources and manifest files.
- **Frida**: A dynamic instrumentation toolkit used to inject scripts into running processes and bypass protections.
- **MobSF (Mobile Security Framework)**: For automated analysis of Android and iOS binaries.
- **Jadx**: A dex-to-java decompiler used to read business logic of Android apps.

Use Case: A loyalty app for a national grocery chain was reverse-engineered to uncover a "hidden" admin API that allowed developers to simulate redemptions. Attackers exploited this to redeem gift cards without deducting actual points.

Botnets and Scripted Emulation

To automate actions at scale — like farming points, simulating user logins, or redeeming daily rewards — attackers often deploy scripted mobile emulators and botnets.

Examples:

- **Android Emulators (e.g., Bluestacks, Nox)**: Scripted using UI automation tools like AutoIt or Appium to mimic human interactions with apps.
- **Custom Bots**: Written in Python, Node.js, or Puppeteer for browser-based loyalty portals.
- **Command-and-Control Botnets**: Used to simulate high-volume but distributed user traffic across global IPs to harvest and cash out loyalty points.

Obfuscation Methods:

- Residential Proxy Rotation to avoid IP bans.
- Human-like Click Delays to bypass behavior analytics.
- Device Fingerprint Spoofing to evade mobile-based detection.

These tools are often sold as fraud-as-a-service (FaaS) packages on dark web marketplaces, complete with documentation, usage support, and performance guarantees.

Use of Dark Web Marketplaces and Forums

The monetization of loyalty fraud occurs across various underground marketplaces, where actors can:

- Buy and sell compromised loyalty accounts.
- Purchase "cash-out configs" for popular loyalty platforms.
- Trade harvested points (e.g., 100k airline miles = $700–$900).
- Offer services for redeeming loyalty points on behalf of clients in exchange for cryptocurrency.

Common Platforms:

- **Exploit.in** – for data dumps and high-volume credentials.
- **Genesis Market** (prior to takedown) – offered browser profiles of compromised loyalty sessions.
- **Telegram channels** – increasingly used to advertise real-time point balances and sale offers.
- **Hydra-style marketplaces** – region-specific platforms for selling stolen loyalty points.

Advanced Social Engineering and AI/ML Abuse

With the rise of AI tools, attackers are now crafting hyper-personalized loyalty-themed phishing campaigns, using:

- **LLM-based phishing generators** to create brand-matching email or SMS content.
- **Image generators** to produce fake loyalty cards or promo banners.
- **Deepfake audio** to impersonate customer support representatives or executive contacts.
- **Synthetic identities** to register accounts en masse and abuse new-user reward programs.

Example: A campaign targeting users of a major online retailer used AI-written emails that mimicked the retailer's voice and color scheme. Victims were led to a phishing page offering "double points day" rewards, which collected credentials and session cookies.

Maturity Scale of Loyalty Fraud Program

Maturity Scale of Loyalty Fraud Program

Incomplete 01	▪ **Lack of Strategy:** No formal fraud prevention strategies or policies in place. ▪ **Minimal Awareness:** Limited awareness of fraud risks among staff and stakeholders. ▪ **Absence of Monitoring:** No monitoring or reporting mechanisms for fraud detection. ▪ **Limited Training:** Little to no training provided to employees on fraud identification. ▪ **Lack of Accountability:** No designated personnel responsible for fraud prevention efforts, leading to a lack of ownership.
Initial 02	▪ **Basic Measures**: Basic fraud prevention measures implemented but inconsistently applied. ▪ **Limited Understanding**: Some awareness of fraud risks, but limited understanding among staff. ▪ **Ad-Hoc Reporting**: Inconsistent reporting processes for fraud incidents, lacking standardization. ▪ **Initial Training**: Training programs for employees are present but not comprehensive or regular. ▪ **Reactive Measures**: Responses to fraud incidents are reactive rather than proactive, with no systematic approach to prevent future occurrences.
Defined 03	▪ **Established Policies:** Documented fraud prevention policies and procedures. ▪ Regular Training: Ongoing training sessions for employees on fraud risks and prevention techniques. ▪ **Defined KPIs:** Key Performance Indicators (KPIs) established for monitoring fraud incidents. ▪ **Cross-Department Collaboration:** Initiated collaboration between departments to address fraud risks collectively. ▪ **Fraud Risk Assessment:** Regular assessments conducted to identify and evaluate potential fraud risks within the organization.
Quantitatively Managed 04	▪ **Data-Driven Approach**: Utilization of analytics and metrics for fraud detection. ▪ **Real-Time Monitoring**: Implementation of real-time monitoring systems for digital and offline channels. ▪ **Trend Analysis**: Regular analysis of fraud trends and vulnerabilities to inform strategy. ▪ **Continuous Improvement**: Established processes for continuous improvement based on performance metrics. ▪ **Incident Reporting System**: Implementation of a standardized incident reporting system that allows for timely and accurate reporting of fraud cases.
Optimized 05	▪ **Advanced Strategies:** Utilization of advanced fraud prevention strategies leveraging machine learning and AI technologies. ▪ **Proactive Threat Intelligence:** Monitoring of the dark web and other sources for proactive threat intelligence. ▪ **Comprehensive Integration:** Full integration of fraud prevention across all business functions. ▪ **Ongoing Optimization:** Continuous optimization of processes and technologies based on emerging threats and best practices. ▪ **Behavioral Analytics:** Utilization of behavioral analytics to detect anomalies fraud patterns in real-time.

Case Studies

Case Studies

This section provides a critical lens through which the practical realities of loyalty program exploitation can be understood. Unlike hypothetical threat models, these real-world incidents reflect the operational blind spots, architectural gaps, and human factors that adversaries exploit.

Each case presented below represents a different attack type — ranging from credential stuffing and API abuse to insider threats and business logic exploitation — across multiple industry verticals.

Major Airline Loyalty Breach – Credential Stuffing & API Abuse	▪ **Organization:** A flagship international airline based in Europe, operating a loyalty program with over 15 million active accounts.
	▪ **Incident Summary:** Between late 2022 and early 2023, the airline's loyalty program experienced a significant wave of unauthorized account access. Customers reported missing miles, unexpected redemptions, and sudden changes to their account profiles. The incident was later confirmed to be the result of a credential stuffing campaign, leveraging leaked username/password combinations from unrelated breaches.
	▪ **Attack Techniques:**
	  ▪ Credential stuffing using OpenBullet configs targeting the airline's loyalty login portal.
	  ▪ Use of rotating residential proxies to bypass geo-based rate limiting.
	  ▪ API abuse after login to redeem miles silently or extract stored PII.
	  ▪ Token reuse allowed session hijacking via weak session scoping.
	▪ **Impact:**
	  ▪ Over 350,000 accounts were accessed without authorization.
	  ▪ Estimated 23 million miles were fraudulently redeemed for gift cards, upgrades, and partner products.
	  ▪ Stolen loyalty data (miles balances and personal info) appeared on dark web forums days after the breach.
	  ▪ Public trust and regulatory scrutiny intensified, forcing the airline to reset all user passwords and notify affected customers.
	▪ **Lessons Learned:**
	  ▪ Loyalty platforms must be protected by multi-factor authentication (MFA), particularly when enabling point redemption or account modifications.
	  ▪ Rate limiting and anomaly detection are critical — even for "non-financial" services.
	  ▪ Session tokens should be scoped to IP and device, and rotated more frequently.

E-commerce Platform Loyalty Fraud – Business Logic Abuse	**Organization:** A rapidly growing online marketplace in North America specializing in electronics and home goods, with a loyalty program offering points for purchases, referrals, and promotions. **Incident Summary:** In 2024, fraud analysts detected a sharp spike in point redemptions for gift cards — with many redemptions originating from new accounts. Deeper investigation uncovered a loophole in the cart abandonment logic, which allowed users to trigger reward points without completing a transaction. **Attack Techniques:** ▪ Users would add items to cart, trigger a promotional flow, and manually intercept the API call that granted reward points. ▪ The cart was then abandoned, and the user would repeat the process with a new account. ▪ Referral links were also exploited — users created self-referral chains using fake emails and temporary inbox services.

	Impact: ▪ Approx. $120,000 worth of gift cards were redeemed over two months. ▪ The fraud ring consisted of just three individuals using mobile emulators and dynamic IP rotation. ▪ The abuse occurred in compliance with apparent business logic, so no fraud alerts were triggered. **Lessons Learned:** ▪ Loyalty platforms must treat business logic validation as a critical part of security testing. ▪ Use of behavioral risk scoring and account activity baselines could have detected the anomaly earlier. ▪ Limiting redemption eligibility for accounts under a certain age or verification level can prevent large-scale abuse.
Grocery Retailer Insider Threat – Unauthorized Point Manipulation	**Organization:** A national grocery retailer in Asia-Pacific operating a widely-used loyalty program linked to phone numbers and payment cards, with in-store redemption at checkout. **Incident Summary:** In Q3 2023, internal audits revealed that several loyalty accounts had unusually high balances and redemption histories that didn't align with customer profiles. The issue was traced to an employee in the loyalty program management team who had been manually adjusting point balances in exchange for cash kickbacks. **Attack Techniques:** ▪ Insider logged into the retailer's internal loyalty admin portal. ▪ Adjusted point balances of dormant accounts to inflate rewards. ▪ Shared access credentials and account information with external co-conspirators. ▪ Gift cards and in-store vouchers were used to launder the rewards. **Impact:** ▪ Financial loss of over $500,000 USD over a 10-month period. ▪ Loyalty program required temporary suspension of redemptions. ▪ Employee terminated; incident led to an overhaul of internal access control policies. **Lessons Learned:** ▪ Loyalty systems need role-based access control (RBAC) and auditing of administrative actions. ▪ Periodic review of point adjustments and outlier redemptions can reveal internal misuse. ▪ Insider threats must be considered in fraud risk frameworks, especially when dealing with systems outside finance.
Retail Pharmacy App Exploited via Mobile Reverse Engineering	**Organization:** A large pharmacy chain with over 2 million monthly app users and a loyalty system tied to medication purchases, wellness challenges, and referral bonuses. **Incident Summary:** Security researchers discovered that the pharmacy's Android app had hardcoded API endpoints and logic for reward calculation. Attackers decompiled the APK, identified a hidden admin-level reward trigger, and replicated its functionality in a custom app that spoofed legitimate behavior. **Attack Techniques:** ▪ APK reverse engineering using JADX and APKTool. ▪ Extraction of a hidden debug API used by internal QA testers. ▪ Mass emulation using Android Studio scripts and emulator farms. ▪ Fake completions of wellness challenges and app milestones.

Impact:

- Over 6 million reward points were fraudulently issued.
- Redemptions for health product vouchers exceeded $80,000 USD.
- Detection occurred only after server anomalies and app telemetry misalignments were observed.

Lessons Learned:

- Developers must remove debug and test code before production releases.
- Secure APIs with environment-specific tokens and scope-limited permissions.
- Use code obfuscation and integrity checks to slow reverse engineering efforts.

Comparative Insights

Case Study	Primary Vector	Attack Techniques	Implication
Airline Loyalty Breach	Credential Stuffing	Proxy rotation, token reuse, API abuse	Weak login & token management
E-commerce Logic Abuse	Business Logic	Cart abandonment abuse, self-referral chains	Poor logic validation, no rate limits
Grocery Retail Insider Threat	Insider Fraud	Manual point adjustments, collusion	No RBAC, lack of audit trails
Pharmacy App Reverse Engineering	Mobile Exploitation	APK decompilation, emulator automation	Hardcoded secrets, no app attestation

Impact of Loyalty Program Fraud

Impact of Loyalty Program Fraud

Loyalty program fraud poses significant risks to organizations, affecting financial stability, customer trust, operational efficiency, and regulatory compliance. The following outlines the key impacts, supported by real-world examples:

Financial Losses: Fraudulent redemptions cause direct losses, with additional indirect costs from investigation and mitigation. For instance, a major airline suffered the loss of over 23 million frequent flyer miles due to a credential stuffing attack in 2022, leading to substantial financial impact. Similarly, a grocery retailer in the Asia-Pacific region lost over $500,000 due to insider fraud involving manual point adjustments.

Reputational Damage: Breaches erode customer trust and damage brand reputation. The Marriott Bonvoy breach (2020–2022) exposed millions of loyalty account records, leading to negative publicity and loss of customer confidence. Such incidents can deter customers from engaging with loyalty programs, reducing their effectiveness.

Operational Disruptions: Detecting and responding to fraud requires significant time and resources, diverting focus from core business operations. For example, the e-commerce platform case in 2024 required extensive fraud analysis to identify a cart abandonment loophole, disrupting normal operations.

Legal and Regulatory Risks: Compromised customer data can lead to legal actions and regulatory penalties under laws like GDPR or CCPA. Organizations may face fines and lawsuits if they fail to protect sensitive information, as seen in cases like the Marriott breach, which prompted regulatory scrutiny.

Indicators of Compromise (IOCs) for Loyalty Fraud

Indicators of Compromise (IOCs) for Loyalty Fraud

Monitoring for indicators of compromise (IOCs) is critical for detecting and preventing loyalty program fraud. The following table lists common IOCs associated with loyalty fraud, along with descriptions and recommended actions:

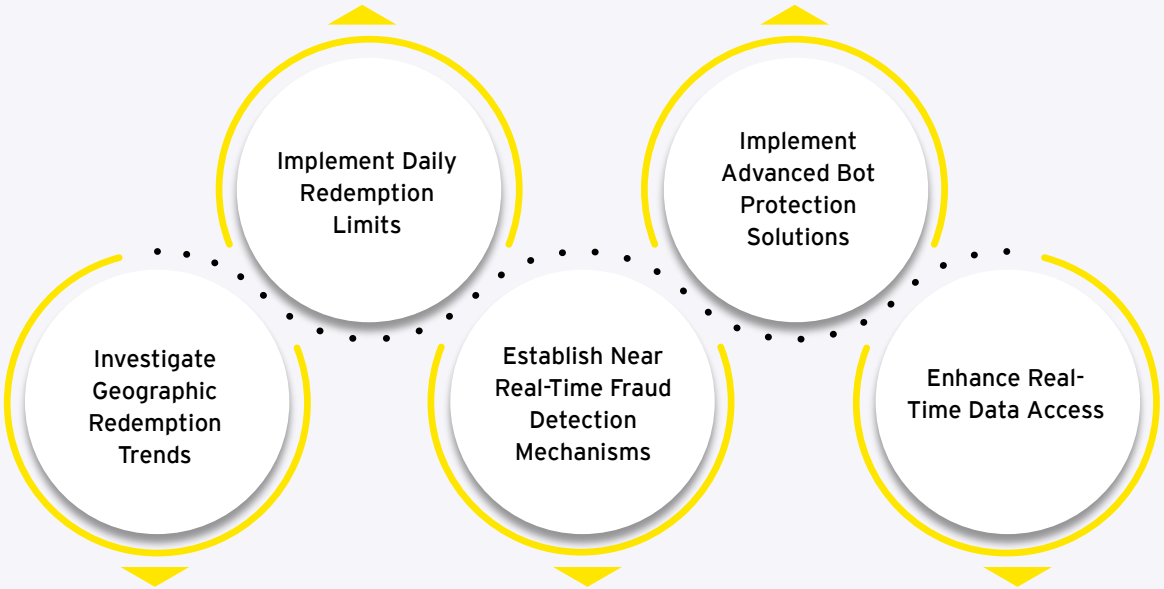
IOC Type	Indicator	Description	Recommended Action
Unusual Login Patterns	Multiple login attempts from different IPs or locations	Indicates potential credential stuffing or account takeover attempts.	Implement rate limiting and monitor for geo-anomalies; enforce MFA.
Sudden Account Activity	Large or frequent point redemptions without corresponding purchase history	Suggests unauthorized access or exploitation of account vulnerabilities.	Set up real-time alerts for unusual redemption patterns; require additional verification.
Compromised Credentials	Use of known breached usernames/passwords from dark web data dumps	Credentials from unrelated breaches used in stuffing attacks.	Use dark web monitoring services to detect compromised credentials; force password resets.
Anomalous Point Transactions	Earning points without purchases or exploiting referral loops	Indicates business logic abuse, such as cart abandonment or self-referral fraud.	Implement behavioral analytics to detect anomalies; validate point-earning transactions.

Industry Best Practices to Combat Loyalty Fraud

Industry Best Practices to Combat Loyalty Fraud

Set a daily cap on the quantity of points that can be redeemed (e.g., $500) to mitigate the financial impact of fraudulent activities. This proactive measure helps to control potential losses and ensures that large-scale fraud attempts are curtailed.

Utilize sophisticated bot protection technologies to detect and block potential automated attacks on the redemption system. This proactive approach helps to safeguard against fraudulent activities that exploit system vulnerabilities.



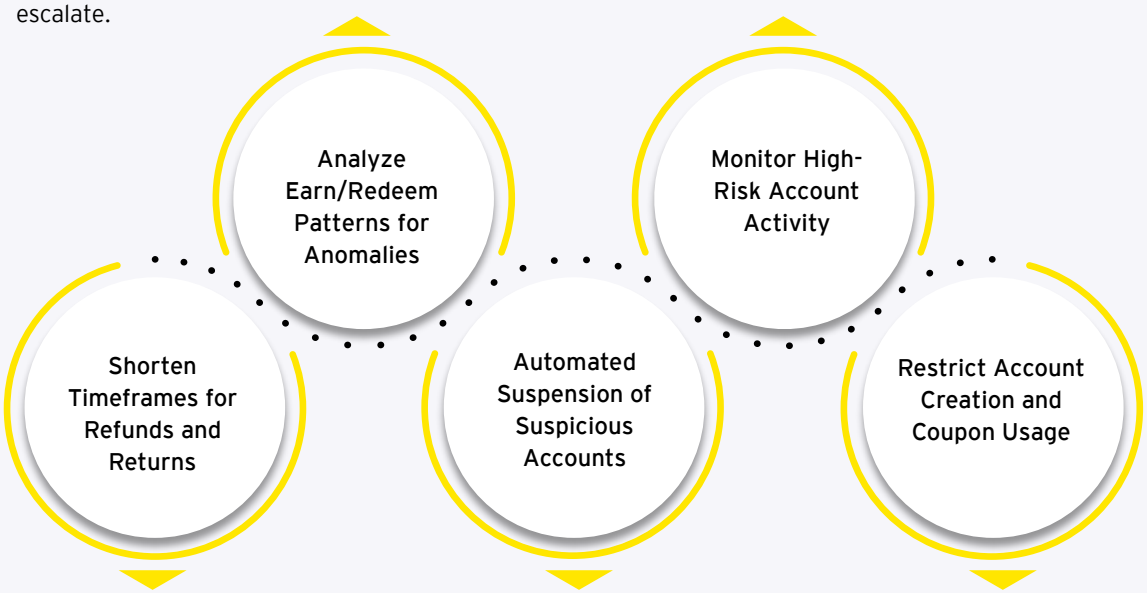
Keep track of where points are being redeemed and look for geographic anomalies. Identifying patterns that deviate from normal behavior can signal potential fraud, allowing for timely intervention and investigation.

Create systems to identify and address fraudulent activities near real-time (minutes/hours) when real-time detection is not feasible. This includes generating manual reports to flag suspicious transactions, allowing for timely intervention and reducing the likelihood of significant losses.

Work closely with the data analytics team to gain immediate access to redemption transaction data. This enables the organization to perform real-time analysis, facilitating quicker decision-making and more effective fraud detection.

Continuously monitor and analyze how points are redeemed to identify unusual or suspicious activity. This includes tracking redemption frequency and amounts, as well as earning points at one location and redeeming points are another location, which can help to uncover potential fraud schemes before they escalate.

Regularly review transactions for redemptions occurring outside the customer's registered home province. This practice helps to identify potentially fraudulent behavior, such as unauthorized use of points in unfamiliar locations, allowing for prompt investigation.



Reduce the period during which points can be refunded or returned after a purchase. By tightening these windows, the organization can minimize the risk of point loss due to fraudulent returns, protecting the integrity of the loyalty program.

Implement a process to suspend accounts that exhibit signs of fraudulent activity after thorough evaluation. This includes generating tickets for further investigation and notifying customers to verify their account activity, thus preventing further point loss.

Limit the number of accounts a single customer can create from one IP address to prevent abuse of the system. This measure helps to reduce the risk of fraudulent sign-ups and ensures that loyalty programs are utilized as intended.

Top Recommendations for Securing Loyalty Programs

Top Recommendations for Securing Loyalty Programs

To protect loyalty programs from fraud and cyber-attacks, organizations should adopt the following measures, tailored to the unique vulnerabilities of loyalty ecosystems:

1. **Implement Multi-Factor Authentication (MFA):** Require MFA for account access and critical actions like point redemptions to prevent unauthorized access. For example, the 2022 airline breach could have been mitigated with MFA.
2. **Use Behavioral Analytics:** Deploy machine learning-based analytics to detect anomalous account activity, such as unusual redemption patterns or login attempts from unfamiliar locations.
3. **Secure APIs:** Protect APIs with OAuth 2.0, rate limiting, and input validation to prevent abuse, as seen in the Marriott Bonvoy API exploitation case.
4. **Conduct Regular Security Audits:** Perform penetration testing and security assessments specifically for loyalty systems to identify vulnerabilities like hardcoded secrets, as exploited in the pharmacy app case.
5. **Educate Customers:** Inform customers about securing their accounts, recognizing phishing attempts, and reporting suspicious activity to reduce social engineering risks.
6. **Monitor Dark Web Activity:** Use threat intelligence services to monitor dark web marketplaces for stolen loyalty credentials, which are often sold at 10–20% of their retail value.
7. **Implement Insider Threat Detection:** Monitor employee activities within loyalty systems to prevent manual point adjustments or collusion, as seen in the grocery retailer case.
8. **Explore Blockchain Technology:** Consider blockchain for secure, transparent point transactions to prevent tampering and enhance trust, an emerging trend in loyalty program security.

These recommendations combine immediate actions with forward-thinking strategies to enhance loyalty program resilience.

Short-Term, Medium-Term, and Long-Term Strategic Response

Short-Term, Medium-Term, and Long-Term Strategic Response

Short Term

In the initial phase, the goal is to close immediate security gaps that could be exploited in credential-based attacks or business logic abuse.

- Enable Multi-Factor Authentication (MFA) for all loyalty accounts to prevent account takeovers, especially after credential stuffing or phishing attempts.
- Set up real-time fraud alerts for suspicious behaviors such as rapid point redemptions, multiple failed logins, or access from unusual locations or devices.
- Conduct a focused security audit of the loyalty platform infrastructure—including mobile apps, APIs, and admin portals—to uncover critical vulnerabilities such as hardcoded secrets, weak authentication, or exposed endpoints.

Medium Term

This phase focuses on building internal capabilities and proactive detection mechanisms, while reinforcing external interfaces like APIs and educating users.

- Deploy machine learning-powered fraud detection tools that can analyze user behavior over time and detect anomalies in account access, point earning, and redemption behavior.
- Strengthen API security using OAuth 2.0, token-based access control, input validation, and rate limiting to block replay attacks, API fuzzing, and abuse of business logic.
- Launch a structured customer education campaign across email, in-app notifications, and help centers—guiding users on securing their accounts, recognizing phishing messages, and reporting suspicious activity.

Long Term

In the long run, the organization should integrate loyalty systems into enterprise security frameworks and embrace innovative technologies that provide operational trust and transparency.

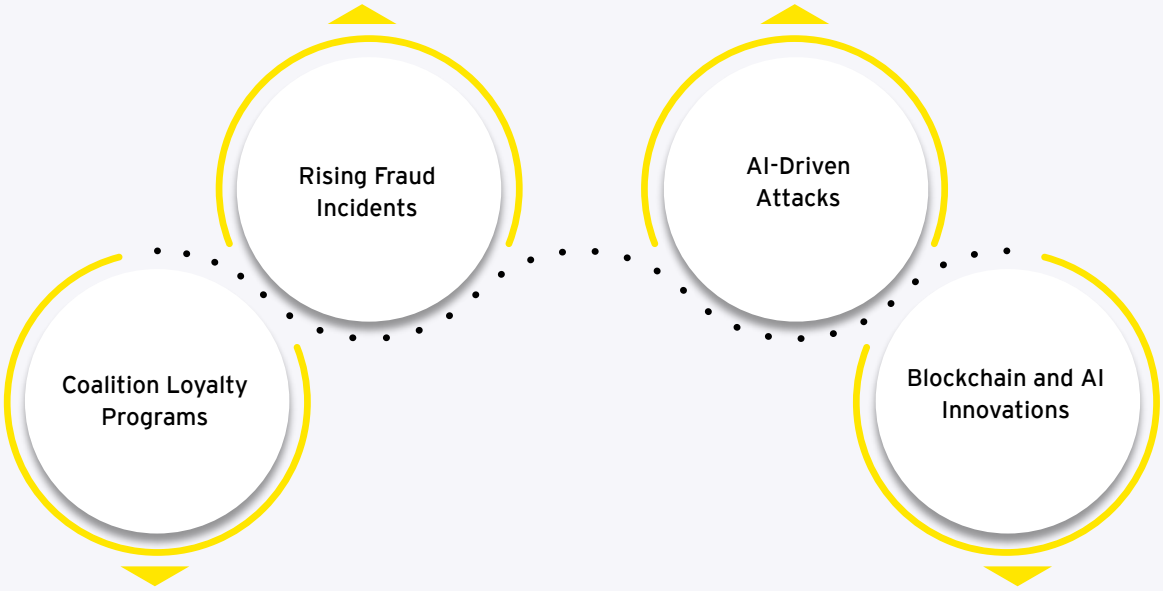
- Align loyalty program security with broader enterprise cybersecurity frameworks, ensuring it's included in security policies, incident response plans, and governance reviews.
- Adopt a Zero Trust Architecture (ZTA) where access is continuously verified, regardless of network origin, and privileges are strictly scoped.
- Partner with external cybersecurity firms and fraud intelligence vendors for persistent monitoring of dark web activity, botnets, and stolen credential resale linked to loyalty programs.
- Explore blockchain and distributed ledger technologies for immutable tracking of point issuance and redemption to enhance auditability, reduce fraud, and build customer trust

Global Trends and Thought Leadership

Global Trends and Thought Leadership

Loyalty program fraud is escalating at a global scale. A 2022 report by Group-IB highlighted a 30% surge in fraud cases, particularly in the airline sector, where millions of frequent flyer miles were compromised. According to Statista (2023), loyalty fraud now constitutes 31% of total fraud attempts against online merchants. This uptick is fueled by attackers leveraging credential dumps, poorly secured APIs, and automated bots. These trends signal that loyalty ecosystems are becoming high-value targets rivaling traditional payment platforms.

The sophistication of phishing, impersonation, and fraud attacks is increasing due to the widespread availability of AI and generative tools. Attackers now use large language models (LLMs) to craft hyper-personalized phishing emails, deepfake voice tools to socially engineer call centers, and automation frameworks to emulate human behavior. As loyalty programs typically lack fraud detection capabilities equivalent to financial systems, they are especially vulnerable to these advanced tactics. Defenses must evolve to detect synthetic behaviors, not just credential mismatches.



The growing popularity of coalition programs—where multiple brands (e.g., airlines, hotels, retailers) pool and share loyalty benefits—offers both benefits and risks. While these ecosystems enhance customer engagement and value, they also increase interconnectivity between platforms, expand the attack surface, and create dependency on third-party security postures. A compromise at one partner can cascade across the coalition. Coordinated security frameworks and shared threat intelligence are becoming essential in managing collective risk.

Emerging technologies like blockchain and distributed ledger systems offer potential for tamper-proof, transparent point transactions, particularly in ecosystems vulnerable to internal fraud or business logic abuse. Meanwhile, AI-driven fraud analytics can profile user behavior across time and channels, detecting anomalies that traditional rule-based systems miss. Leading retailers are piloting these technologies to establish verifiable point issuance, immutable transaction logs, and real-time behavioral scoring—positioning themselves as pioneers in trust and transparency.

Resources

Resources

Title	Description	Source
2024 Verizon Data Breach Investigations Report (DBIR)	Annual industry-wide analysis of breach trends, including credential stuffing and retail-specific fraud vectors.	https://www.verizon.com/business/resources/reports/dbir/
ENISA Threat Landscape 2023	Comprehensive review of cyber threat trends in Europe, covering retail, e-commerce, and loyalty fraud.	https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
FBI Internet Crime Report 2023	Official statistics on cybercrime incidents in the U.S., including BEC, gift card, and loyalty fraud.	https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
MITRE ATT&CK Framework	Global knowledge base of adversarial tactics and techniques, used for threat mapping and defense alignment.	https://attack.mitre.org/
OWASP API Security Top 10 – 2023	Authoritative list of API threats including business logic abuse, rate limiting, and token mismanagement.	https://owasp.org/API-Security/
Airline Loyalty Breach: BleepingComputer	Report on credential stuffing attacks that compromised millions of airline loyalty accounts.	https://www.bleepingcomputer.com/news/security/airline-mileage-accounts-hacked-in-credential-stuffing-attacks/
Gift Card Fraud on the Rise – ThreatPost	Insight into bot-driven fraud targeting gift card and loyalty redemption workflows.	https://threatpost.com/gift-card-fraud-bots/174414/
AI Voice Deepfakes Targeting Call Centers	Explains how attackers use AI-generated voices to exploit customer service workflows.	https://www.wired.com/story/voice-deepfakes-ai-scams/

Title	Description	Source
Selling Loyalty Points on Dark Web – Flashpoint	Threat intelligence on how stolen loyalty credentials are traded in cybercrime forums.	https://www.flashpoint.io/blog/loyalty-program-abuse-dark-web/
Synthetic Identity Fraud – Sift Report	Breakdown of referral abuse and synthetic accounts used to farm loyalty rewards.	https://sift.com/resources/reports/q2-2023-digital-trust-safety-index
Credential Stuffing with OpenBullet – Cybernews	Explains how tools like OpenBullet are used in automated attacks on login portals.	https://cybernews.com/security/openbullet-tool-credential-stuffing/
Arkose Labs Fraud and Abuse Report	Trends in bot-based loyalty abuse and emulator-based automation tactics.	https://www.arkoselabs.com/resource/2023-fraud-and-abuse-report/
Check Point Security Report 2024	Global report including analysis on botnet use in reward system attacks.	https://www.checkpoint.com/downloads/product-related/security-report-2024.pdf
Jumio Identity Fraud Research 2024	Research on KYC circumvention and fake document generation in loyalty signups.	https://www.jumio.com/resources/identity-fraud-report/
IBM Cost of a Data Breach Report 2024	Industry benchmarks on the financial and reputational impact of data compromise.	https://www.ibm.com/reports/data-breach
Gartner Market Trends – Loyalty Fraud	Strategic guidance on fraud evolution in digital loyalty programs and mobile wallets.	https://www.gartner.com/en/documents/4000201
Cisco Talos: API Attacks on Retail	Insights into insecure API exploitation in commerce and loyalty systems.	https://blog.talosintelligence.com/api-abuse-retail/
Forbes – The $200 Billion Loyalty Economy	Business case for loyalty programs as financially significant digital assets.	https://www.forbes.com/sites/blakemorgan/2023/10/18/the-200-billion-loyalty-economy/

Title	Description	Source
TechCrunch: Loyalty Program Breaches	News coverage on incidents involving compromised reward accounts and user data.	https://techcrunch.com/tag/loyalty-program/
Cybersecurity Ventures: Retail Fraud Forecast	Projections on global cybercrime impact on sectors including retail and rewards systems.	https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
ThreatPost: Loyalty Bot Attacks	Detailed overview of automated bots used to drain loyalty points across platforms.	https://threatpost.com/loyalty-programs-bot-attacks/172512/
Wired: API Security Gaps	Exploration of overlooked API vulnerabilities in consumer-facing digital services.	https://www.wired.com/story/api-security-risks-retail/
McKinsey & Company. (2022). Loyalty Economics Report	Estimates $200 billion in unredeemed rewards globally.	https://www.mckinsey.com
Statista. (2023). Dark Web Digital Products Price Stats	Average price of selected illegal digital products for sale on the dark web.	https://www.statista.com/statistics/1275187/selling-price-illegal-digital-products-dark-web/
Forbes. (2019). Are Loyalty Points Replacing Bitcoin?	Examines how loyalty points are being used as a dark web currency.	https://www.forbes.com/sites/forbestechcouncil/2019/05/23/are-loyalty-points-replacing-bitcoin-as-the-favored-dark-web-currency/
Group-IB. (2023). Airline Loyalty Program Fraud	Reports on a 30% increase in airline loyalty fraud.	https://www.infosecurity-magazine.com/news/airlines-battle-loyalty-program/
DataDome. (2024). Loyalty Fraud Guide 2025	Detailed strategies for detecting and preventing loyalty fraud.	https://datadome.co/learning-center/loyalty-fraud/

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2025 EYGM Limited.

All Rights Reserved.

ED None.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com