Unmasking loyalty scheme fraud

An inside look and your ultimate guide to fighting back

June 2024

EY

Building a better working world

Introduction and Current Situation

Loyalty programs are a pivotal strategy for many companies, playing a crucial role in customer retention and revenue growth. They reward customer engagement with points, miles or some form of cash incentive, often exchangeable for goods or services, thereby transforming customer satisfaction into brand loyalty.

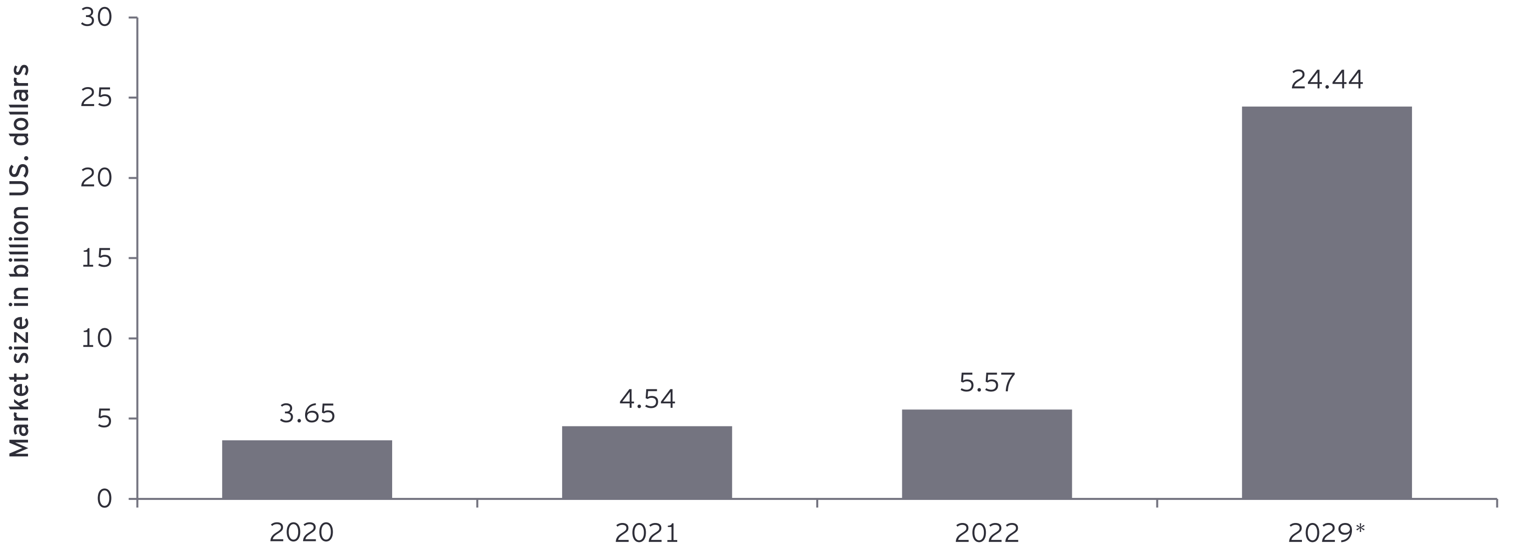
However, these same benefits can attract undesired attention, making these programs an attractive target for fraudsters. The consequential damage from these fraudulent activities can be significant, extending beyond tangible financial loss to diminished customer trust and harm to the company's reputation.

Loyalty fraud is a growing problem across the globe, and Canada is no exception. Canadian consumers have one of the highest per-capita participation rates in loyalty programs, which makes these programs attractive targets for fraudsters. The situation has only worsened with the significant shift towards online shopping due to the COVID-19 pandemic. With more transactions happening online, the opportunities for digital fraud, including loyalty fraud, have increased.

Loyalty programs are attractive to fraudsters because they are often less secure than other types of accounts, and both the companies and customers may not monitor them as carefully. As a result, the financial losses from loyalty program fraud – both direct and indirect – are escalating at a worrying pace, with current estimates suggesting an annual financial loss of $1 billion.

Despite fraud prevention measures being implemented, the problem persists as the safeguards put in place for these programs often do not match the level of rigor employed for primary financial systems. Therefore, it is imperative that businesses remain vigilant and proactive in protecting their customers and their brand reputation from loyalty fraud.

Loyalty management market size worldwide from 2020 to 2029
(in billion U.S. dollars)



© Statista 2024

Common Types Of Loyalty Fraud

ACCOUNT TAKEOVER

Account takeover, prevalent in the realm of loyalty fraud, typically involves fraudsters unlawfully gaining access to a user's loyalty program account. Techniques often used for this include phishing, deploying malware or initiating brute force attacks. Once access is established, fraudsters manipulate the account for their benefits, usually by unlawfully redeeming points for gift cards or buying merchandise.

REDEMPTION FRAUD

Redemption fraud within loyalty programs entails illegitimate practices where fraudsters unlawfully obtain control over an individual's rewards account and redeem the accrued points or rewards without consent. In the context of online transactions, this type of fraud involves cybercriminals exploiting techniques such as phishing, data breaches, or other cybersecurity attacks to gain unauthorized access to loyalty reward accounts. Once inside, they swiftly redeem accumulated points or rewards for various options, such as online purchases, e-gift cards, or travel rewards. Conversely, in a physical store environment, fraudsters can redeem stolen points by either cloning the loyalty card or barcode or physically stealing the card. In some cases, compromised point-of-sale systems can aid criminals in executing this type of fraud in retail establishments.

DATA BREACH

When a loyalty program's database is breached, a significant risk emerges as cybercriminals might gain unauthorized access to confidential client data. Such data can include sensitive details, including loyalty account credentials and specific account information. This unauthorized access opens up a backdoor for criminals, equipping them with classified information to be used for illicit purposes. For instance, they could exploit these credentials to make unauthorized transactions, redeem rewards, alter account details, or even sell these credentials on the black market. In certain cases, they can use the obtained personal data for more advanced crimes such as identity theft. This unlawful accessibility presents a significant threat to both the customers and the business, leading to potential financial losses, a breach of trust, and reputational damage.

POLICY ABUSE

Policy abuse encapsulates actions that involve exploiting a system's established rules or guidelines for illegitimate gain. It often involves acts that may not technically be illegal but are considered unethical or against the intent of the policy. In the context of loyalty programs, policy abuse could include practices such as creating an excessive number of bogus accounts to capitalize on introductory bonuses or offers. It might also involve exploiting loopholes in a program's terms and conditions to accumulate an unusually high volume of reward points or discounts. This could entail behaviours such as making large purchases to earn points and then returning the items while retaining the rewards. Other tactics may include 'gaming' referral systems by referring fictitious customers or continually cancelling and rebooking services to exploit initial booking perks. Such forms of policy abuse can undermine the economic viability of the loyalty program, create an unfair environment for genuine customers, and potentially damage the reputation of the business.

EMPLOYEE OR INSIDER FRAUD

Insider fraud involves fraudulent activities committed by employees or individuals who have a deeper understanding of the loyalty program's workings. These individuals capitalize on system vulnerabilities, bypass controls, or misuse their privileged access rights to steal reward points, personally identifiable information, or tamper with member accounts. Due to their intimate knowledge of system operations and their access rights, these insiders carry out manipulations that are socially harmful and often difficult to identify. They can carry out subtle yet substantial alterations to the system, granting them undue benefits. Additionally, the fact that they may steal sensitive personally identifiable information exacerbates the situation further as it could lead to more serious implications involving identity theft, potential legal issues, and severe breaches of customer trust.

Risks Of Loyalty Fraud

Financial loss

The unauthorized use or theft of points in loyalty programs can rapidly deplete an organization's resources, leading to substantial monetary losses. Moreover, these illicit redemptions can disrupt the normal functioning of the loyalty program, causing further financial strain on the business.

Trust erosion

A decrease in customer trust, often a result of fraudulent activities, can lead to reduced participation in loyalty programs. This drop in engagement can hinder business growth and potentially impact overall customer loyalty.

Brand damage

Fraudulent activities can seriously damage a brand's reputation, tarnishing its public image. This could potentially lead to loss of customer trust and loyalty, making it harder to attract new customers.

Operational disruptions

Operational disruptions can arise when resources must be redirected to handle fraud cases, rectify vulnerabilities and support impacted customers. This diversion can impact regular operations, potentially resulting in reduced efficiency and productivity.

Service Costs

Increased customer service costs can arise as businesses have to handle more inquiries from customers affected by fraud. The extra resources necessary to accommodate these inquiries can lead to higher operational costs.

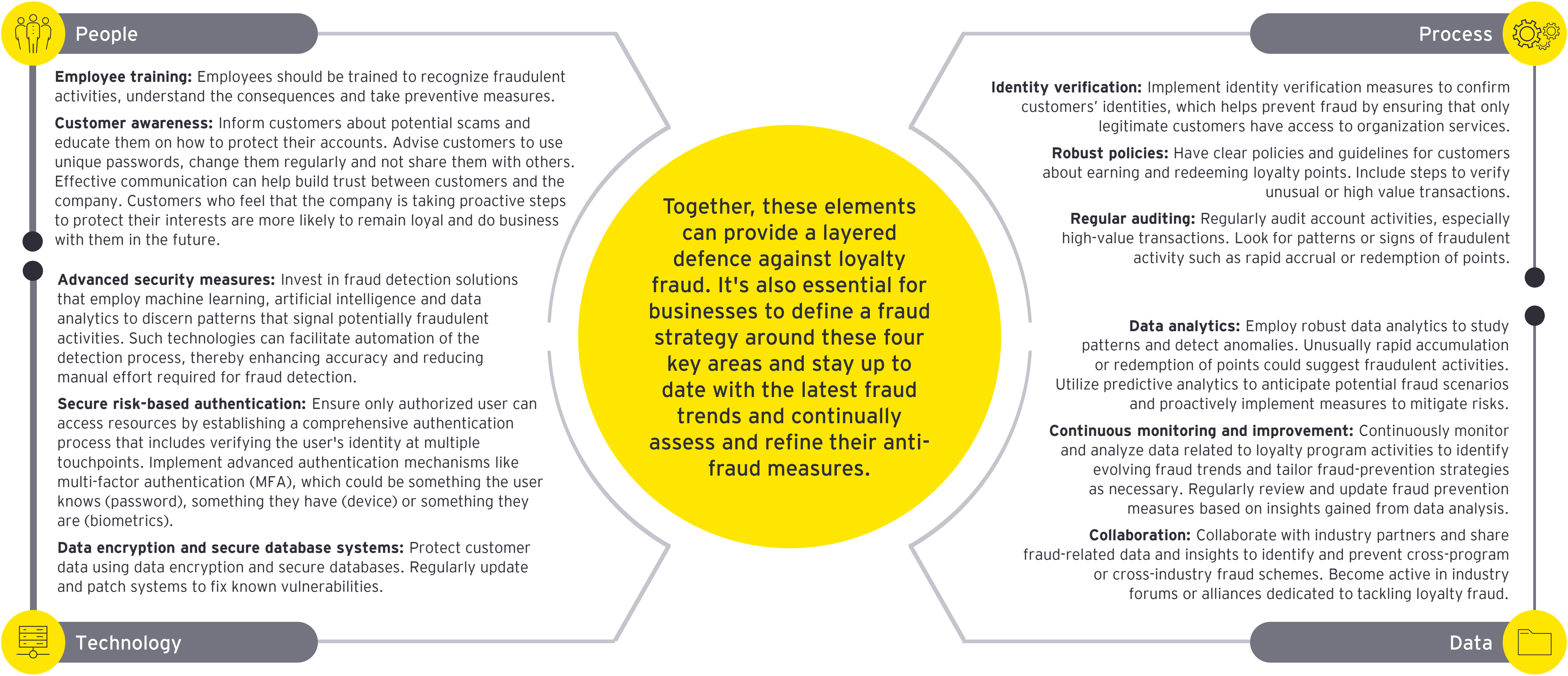
Partnership Risks

The risk of business partners severing collaborations can heighten if fraud issues jeopardize their customer relationships or reputation. This disruption can have significant consequences for the business's operations and its network of partnerships.

Legal Consequences

Fraudulent activities can lead to serious legal implications. Depending on the scale and nature of the fraud, businesses could face hefty fines, lawsuits or even criminal charges.

How Companies Can Tackle Loyalty Fraud



People

Employee training: Employees should be trained to recognize fraudulent activities, understand the consequences and take preventive measures.

Customer awareness: Inform customers about potential scams and educate them on how to protect their accounts. Advise customers to use unique passwords, change them regularly and not share them with others. Effective communication can help build trust between customers and the company. Customers who feel that the company is taking proactive steps to protect their interests are more likely to remain loyal and do business with them in the future.

Technology

Advanced security measures: Invest in fraud detection solutions that employ machine learning, artificial intelligence and data analytics to discern patterns that signal potentially fraudulent activities. Such technologies can facilitate automation of the detection process, thereby enhancing accuracy and reducing manual effort required for fraud detection.

Secure risk-based authentication: Ensure only authorized user can access resources by establishing a comprehensive authentication process that includes verifying the user's identity at multiple touchpoints. Implement advanced authentication mechanisms like multi-factor authentication (MFA), which could be something the user knows (password), something they have (device) or something they are (biometrics).

Data encryption and secure database systems: Protect customer data using data encryption and secure databases. Regularly update and patch systems to fix known vulnerabilities.

Together, these elements can provide a layered defence against loyalty fraud. It's also essential for businesses to define a fraud strategy around these four key areas and stay up to date with the latest fraud trends and continually assess and refine their anti-fraud measures.

Process

Identity verification: Implement identity verification measures to confirm customers' identities, which helps prevent fraud by ensuring that only legitimate customers have access to organization services.

Robust policies: Have clear policies and guidelines for customers about earning and redeeming loyalty points. Include steps to verify unusual or high value transactions.

Regular auditing: Regularly audit account activities, especially high-value transactions. Look for patterns or signs of fraudulent activity such as rapid accrual or redemption of points.

Data

Data analytics: Employ robust data analytics to study patterns and detect anomalies. Unusually rapid accumulation or redemption of points could suggest fraudulent activities. Utilize predictive analytics to anticipate potential fraud scenarios and proactively implement measures to mitigate risks.

Continuous monitoring and improvement: Continuously monitor and analyze data related to loyalty program activities to identify evolving fraud trends and tailor fraud-prevention strategies as necessary. Regularly review and update fraud prevention measures based on insights gained from data analysis.

Collaboration: Collaborate with industry partners and share fraud-related data and insights to identify and prevent cross-program or cross-industry fraud schemes. Become active in industry forums or alliances dedicated to tackling loyalty fraud.

Final Thoughts

While loyalty programs are essential tools for driving customer retention, they cannot be effectively employed without proper safeguards against burgeoning fraud risks. Implementing a broad approach that includes people, process and technological controls can create a balanced and secure environment.

Helping ensure the integrity of your loyalty program is not merely about preventing financial loss. It's about maintaining your customers' trust and your brand's reputation. We're committed to helping you safeguard your loyalty program through our highly integrated suite of services.

Let's explore how you can bolster your defences against loyalty fraud.

Contact us

Ramzi Bou Hamdan

PARTNER, FINANCIAL CRIME RISK CONSULTING

EY Canada

+1 647 616 8727

Ramzi.BouHamdan@ca.ey.com

Mathieu Auger-Perreault

PARTNER, FRAUD RISK CONSULTING LEADER

EY Canada

+1 514 490 2263

mathieu.auger-perreault@ca.ey.com

Taher Talib

MANAGER, FRAUD RISK CONSULTING

EY Canada

+1 587 707 1853

Taher.Talib@ca.ey.com

Elie Al-Chartouni

STAFF, FRAUD RISK CONSULTING

EY Canada

+1 416 932 4115

Elie.Al-Chartouni@ca.ey.com

References and appendices

“50 Stats That Show The Importance Of Good Loyalty Programs, Even During A Crisis”

Blake Morgan, Forbes, May 7, 2020,

https://www.forbes.com/sites/blakemorgan/2020/05/07/50-stats-that-show-the-importance-of-good-loyalty-programs-even-during-a-crisis/?sh=3e48832c2410

“Why Rewards for Loyal Spenders Are ‘a Honey Pot for Hackers”

Tiffany Hsu, The New York Times, May 11, 2019,

https://www.nytimes.com/2019/05/11/business/rewards-loyalty-program-fraud-security.html

“Loyalty management market size worldwide from 2020 to 2029”

Julia Faria, Statista, July 18, 2023,

https://www.statista.com/statistics/1295852/loyalty-management-market-size-world

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

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.

4483373
ED 0000

This publication contains information in summary form, current as of the date of publication, and is intended for general guidance only. It should not be regarded as comprehensive or a substitute for professional advice. Before taking any particular course of action, contact EY or another professional advisor to discuss these matters in the context of your particular circumstances. We accept no responsibility for any loss or damage occasioned by your reliance on information contained in this publication.

ey.com/en_ca