CyberSource®
the power of payment

LOYALTY FRAUD IN RETAIL ECOMMERCE

Manage fraud in the customer loyalty lifecycle

Published May 2017

www.cybersource.com/asiapacific

INTRODUCTION

Online retail merchants use loyalty or rewards programmes with the aim to provide a more pleasant and thoughtful shopping experience that is closely associated with their brand, and turn customers into faithful followers and regular buyers.

Deploying digital rewards is a viable option thanks to the lower cost, convenience, and higher perceived value. However, as with anything of value and mobility, digital rewards have become a keen target for fraudsters. Given that loyalty members contribute the bulk of a merchant's sales, loyalty fraud detection and prevention is essential to protecting the bottom line.

This CyberSource whitepaper will help merchants understand the key considerations, and the appropriate mitigation techniques and tools when implementing a loyalty fraud management strategy. Of course, this strategy should be aligned vis-à-vis the merchant's overall fraud management strategy across various payment channels and customer touch points.

Andrea Tan
Director, Business Solutions & Segments,
CyberSource Asia Pacific

Loyalty Rewards Tempt Customers…and Fraudsters

Reward points or dollars may not be real money, but they function just like currency, carrying monetary value such as gift redemptions, discounts, rebates or cashback vouchers.

The monetary value is meant to draw customers into becoming loyal spenders, though it is equally enticing to fraudsters who exploit this channel to steal loyalty data and points, usually by exploiting account loopholes, hacking data sources or gaming the programme.

Individuals or groups who commit loyalty fraud are not always necessarily organised criminals or computer hackers. Perpetrators could also be employees who manipulate the points from inside the system, or loyalty members who attempt to cheat the programme to get points, discounts, or redemptions without fulfilling the qualifications.

Despite the risks, loyalty programmes are proven to boost sales, customer satisfaction and business reputation. According to Nielsen, 72% of consumers globally—and even more in Asia Pacific (78%)—say they will choose to buy from a retailer with a loyalty programme over one without[1]. Another survey done by Forrester found that the average loyalty membership rate is about nine programmes[2] per person.

The prevalence of loyalty programmes is set to keep rising, as brands seek to create or strengthen customer communities, especially during times of challenging economic conditions and fickle consumer sentiment.

So, as digital loyalty programmes evolve from a routine marketing tactic to a strategic competitive differentiator, merchants will invest in new or enhanced programmes, which in turn increases the value of loyalty currency to customers. This, however, inevitably heightens the risks of loyalty fraud as well.

[1] Nielsen, "Allegiant Alignment: What Faithful Followers of Retail Loyalty Programs Want." Nov 2016. http://www.nielsen.com/sg/en/insights/news/2016/allegiant-alignment-what-faithful-followers-of-retail-loyalty-programs-want.html

[2] Forrester, "North American Consumer Technographics Customer Lifecycle Survey 2", Q3 2014.

LOYALTY FRAUD:
A Different Challenge From Payment Fraud

It is important merchants understand that loyalty fraud is not managed the same way as payment fraud. That is because payment fraud strikes mainly at the checkout stage, whereas loyalty fraud infiltrates the customer's buying journey much more fluidly.

This type of fraud can creep in at any one or more areas along the entire customer loyalty journey—at account creation or access before a purchase, during payment at checkout, or at post-purchase redemption—which gives fraudsters more avenues and opportunity. Here are a few scenarios:

- Fraudster creates a fake loyalty account and takes over a genuine customer's loyalty account, transferring all the points to the fake account. The goal may either be to redeem a lot of free merchandise or sell the points for cash.
- Fraudster hacks a customer's shopping account and deliberately makes big, expensive orders for delivery to that victim's shipping address. That's because the intention all along was to steal the earned loyalty points before either victim or merchant realises the con.
- Fraudster takes over a loyalty customer's account to get access to other valuable personal data such as email, phone number, address, password, and payment details. Armed with this data, the fraudster can hack other accounts belonging to the same customer, steal payment credentials, and run identity scams—all while milking the fact that between 31% and 55% of people use the same password at multiple sites[3].

Merchants would never ignore or downplay payment fraud in running their business. In the same vein, they should not dismiss loyalty fraud. Furthermore, loyalty accounts are a tempting alternative in the eyes of fraudsters. This is because loyalty accounts are, to some extent, easier to target compared to online payment channels, due to the following reasons:

- Unlike bank or credit card accounts, customers may not check their loyalty accounts as often, especially if they have too many to remember. What's left is a vault of unredeemed points in often dormant accounts.
- Merchants may deploy fewer or no controls to mitigate loyalty fraud, unlike online payment fraud with which they are more familiar and tend to invest most of their budget and resources.
- Rewards currency at present is not well-covered by financial regulations with comprehensive and cohesive liability protection—something fraudsters will readily exploit at the merchant's expense.

[3] Center for Internet Security, "Reusing Passwords on Multiple Sites", Jun 14, 2016. https://blog.cisecurity.org/reusing-passwords-at-multiple-sites

THE HIGH COSTS
of Loyalty Fraud

LOSS OF REVENUE

The financial implications of loyalty fraud attacks cannot be underestimated. Loyalty currency contains value to redeem products or services of value, and exist as liabilities on the merchant's balance sheet. Hence, any fraudulent use of the points would mean a write-off on the balance sheet, which in turn impacts margins.

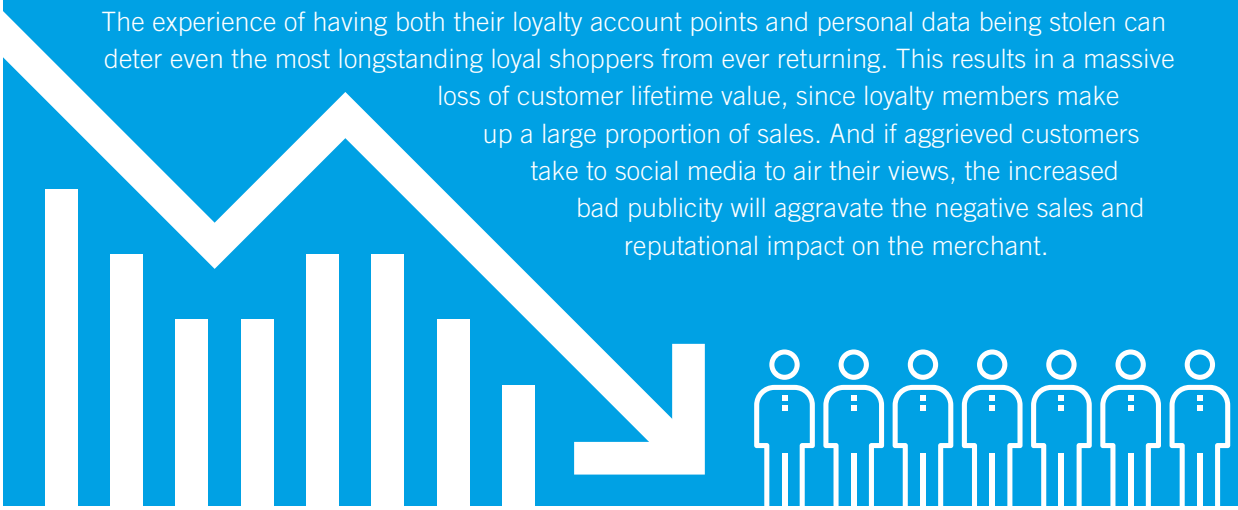
As an example, reward redemptions typically require a minimum or tiered amount of points with the purpose of encouraging shoppers to spend more to meet the criteria. If the loyalty points used in redemption were stolen or purchased illegally, then the exchanged monetary items—whether it is merchandise, rebates or cash vouchers—will be counted as losses in the merchant's revenue books. If reward points were awarded to purchases made with fraudulent cards, the merchant is hit twice with chargeback losses.

LOSS OF CUSTOMER TRUST AND REPUTATION

Research from Forrester found that one in four shoppers aged between 18 years and 34 years are willing to share their personal data to get exclusive discounts[4]. Merchants, on their end, want personal data to understand their best customers in the loyalty database better. Foremost in this exchange of personal information between the two parties is trust.

Theft or illegal use of loyalty account points is often linked to a massive data breach of sensitive user information. When that happens, it is not just customer trust that gets eroded, but merchant reputation and brand value as well.

The experience of having both their loyalty account points and personal data being stolen can deter even the most longstanding loyal shoppers from ever returning. This results in a massive loss of customer lifetime value, since loyalty members make up a large proportion of sales. And if aggrieved customers take to social media to air their views, the increased bad publicity will aggravate the negative sales and reputational impact on the merchant.



[4] Forrester, "North American Consumer Technographics Customer Lifecycle Survey 2", Q3 2014.

HOW TO MITIGATE
Loyalty Fraud

MANAGEMENT THROUGHOUT THE CUSTOMER LIFECYCLE

Loyalty programmes are designed to nurture customer relationships, so they are never confined to a single, isolated activity. This ongoing customer engagement forms a journey otherwise known as the customer loyalty lifecycle.

Defending the entire loyalty chain is imperative because fraudsters will keep looking for loopholes and vulnerabilities to exploit at one or more stages along the lifecycle. For example, they might use multiple different devices in an attempt to log in to an account within a short time, make multiple transfers of points into an account, or link other persons to a loyalty account via new devices.

The **CyberSource Loyalty Fraud Management Solution** protects a merchant's revenue and best customers by accurately detecting and stopping fraudulent behaviours throughout the loyalty lifecycle—from points purchase and account creation to redemption, and all other activities in between, such as incremental or sudden points increase.

The solution equips merchants with two major capabilities that will strengthen defence and reduce risk in their loyalty programmes:

ACCOUNT MONITORING

Account Takeover Protection is the first line of defence by identifying fraud at account creation and login, while monitoring for suspicious account changes.

Consumers use multiple devices to make purchases and earn points, so merchants need intelligent technology in scanning behavioural changes to distinguish between valuable returning customers and fraudulent account creation or account takeover attempts.

TRANSACTION SCREENING

Decision Manager screens for fraud at the point of transaction or checkout, to protect purchase or redemption of loyalty points.

As the world's largest fraud detection radar, Decision Manager increases fraud pattern visibility by 200X, and evaluates hundreds of data elements to detect fraud accurately with or without credit card information since loyalty transactions may not involve standard payment types.

Get additional support from **CyberSource Managed Risk Services**

Complement your fraud management tools and capabilities with CyberSource fraud experts or scale your expertise and capacity without adding fixed headcount. Our fraud analysts provide consultation on fraud prevention configuration, best practices and industry strategies to help ensure that fraud rates are kept low, while operations are kept efficient.

Complement your in-house skills and resources with the global team of CyberSource fraud management experts. Managed Risk Analysts, who serve clients on five continents, can help you optimise Decision Manager and scale operations. This network of experts can help you identify new fraud trends before they affect your business.

Protect Your Customer Relationships, **PROTECT YOUR PROFITS**

Loyalty programmes are one of the most effective ways merchants can use to increase the volume of repeat customers and revenue. The loyalty points themselves may not be legal tender; but as loyalty currency they entail monetary benefits that are tied to sales and profit margins, and hence require adequate, holistic loyalty fraud management. Otherwise, a business risks letting loyalty fraud destroy the very thing the loyalty programme was designed for.

With the **CyberSource Loyalty Fraud Management Solution**, you can grow your loyalty programme to boost customer retention and brand loyalty without fear of fraud.

CyberSource, a wholly owned subsidiary of Visa Inc., is the only integrated payment management platform built on secure Visa infrastructure, with the payment reach and fraud insights of a massive $358Bn global processing network. CyberSource and Authorize.Net payment management solutions help 475,000 large and small businesses grow sales, mitigate risk, and operate with greater agility. CyberSource operates globally, and is headquartered in San Francisco, California and maintains offices throughout the world, with regional headquarters in Singapore, Tokyo, Miami / Sao Paulo and Reading, U.K.

For more information, please visit **www.cybersource.com/asiapacific**

ASIA PACIFIC

Asia Pacific CYBS Singapore Pte Ltd
Phone: 01-800-6671-5000 (Singapore / Thailand)
Phone: 00-800-6671-5000 (Malaysia)
Phone: 000-800-630-1003 (India)
Phone: 1-800-8-756-8388 (Philippines – Globe)
Phone: 1-800-10-802-7222 (Philippines – PLDT)
Email: ap_enquiries@cybersource.com
Website: www.cybersource.com/asiapacific

CyberSource Australia & New Zealand
Phone: 0011-800-6671-5000 (Australia)
Phone: 00-800-6671-5000 (New Zealand)
Email: anz_enquiries@cybersource.com
Website: www.cybersource.com.au

CYBS Greater China
Email: gc_enquiries@cybersource.com
Website: www.cybersource.com/cn

CyberSource KK (Japan)
Phone: +81 3 3548 9873
Email: sales@cybersource.co.jp
Website: www.cybersource.co.jp

LATIN AMERICA & CARIBBEAN

CyberSource Miami
Email: lac@cybersource.com
Website: www.cybersource.com/lac

CyberSource Mexico
Email: mexico@cybersource.com
Website: www.cybersource.com.mx

CyberSource Brazil
Email: brasil@cybersource.com
Website: www.cybersource.com/brasil

NORTH AMERICA (US & Canada)

CyberSource Corporation HQ
Email: sales@cybersource.com
Website: www.cybersource.com

EMEA (Europe, Middle East & Africa)

CyberSource EMEA
Email: uk@cybersource.com
Website: www.cybersource.com/emea

CyberSource Visa Middle East FZ-LLC
Website: www.cybersource.com/mea

www.cybersource.com/asiapacific

LFRWP/201703