EXECUTIVE BRIEF | MAY 2015

ca technologies

How Do I Keep My Loyalty Programs Secure From Breaches While Retaining My Member Loyalty?

Reduce Financial Losses And Increase Member Confidence By Protecting Your Loyalty Programs From Hackers.

The Nielsen Global Survey of Loyalty Sentiment polled more than 29,000 Internet respondents in 58 countries to evaluate consumer views on loyalty levels across 16 categories, ranging from consumer goods staples to technology products to retail and found that, nearly 59 percent of all respondents claimed that loyalty programs were available for participation with the retailers where they had shopped. The demand for loyalty programs is exceedingly high for consumers, with about 84 percent of respondents stating that they were more likely to choose retailers that offered a loyalty program.

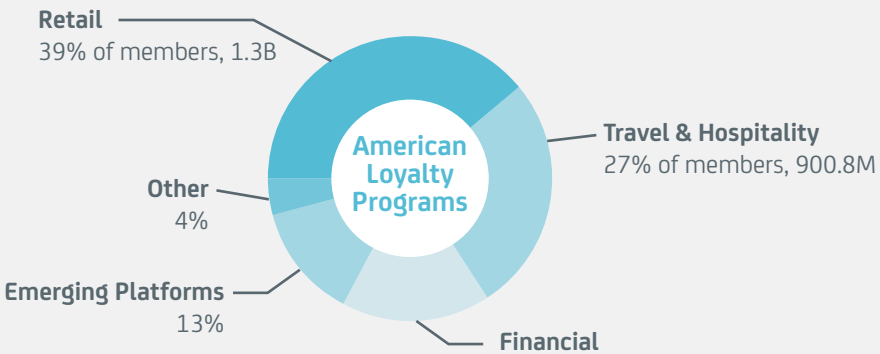
However, these same loyalty programs have become a huge target for hackers to fraudulently access member's accounts and steal their hard-earned points. Online loyalty portals typically have a weak security infrastructure. Combine this with the fast-growing market for the tangible value of stolen reward points, and undesired pain points for companies that offer loyalty programs are created. Companies face real out-of-pocket cost when they have to pay for an item that was purchased by a fraudster. Members can also lose confidence in both the brand and loyalty program, which may cause them to opt for a competitor's program if there is not a strong sense of security or user-friendliness. Companies must walk a fine line in order to offer a loyalty program that members find beneficial and make sure that both the company and members are secure against malicious attacks.

Security Challenges for Loyalty Programs

The ever-evolving landscape of hacking drives companies across all loyalty sectors—retail, financial services and travel/hospitality—to quickly adapt and invest in new approaches to securing their loyalty programs as well as protecting their members' points and private information. A majority of companies have already realized that security needs to be a top priority if they desire to remain competitive in the marketplace and retain their member's loyalty.

Loyalty Program Stats

1 American Loyalty Program memberships jumped 26%, to 3.3B, from 2012-2014 (2.6B).



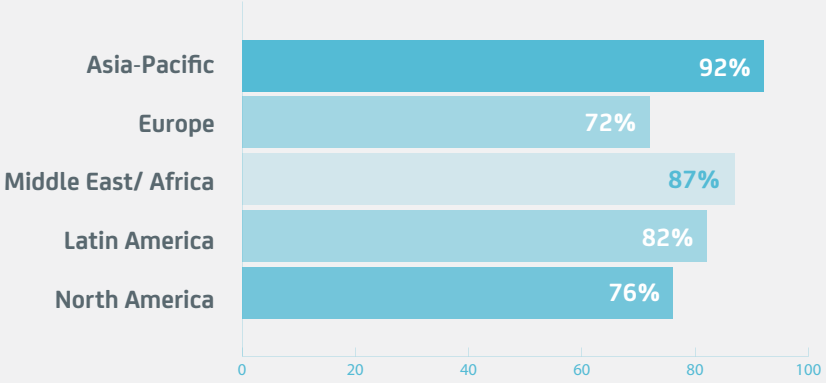
Source: Colloquy Report

2 Loyalty Programs must have a holistic customer experience and embrace innovative technology to deliver seamless services and interactions.

Source: Colloquy Report

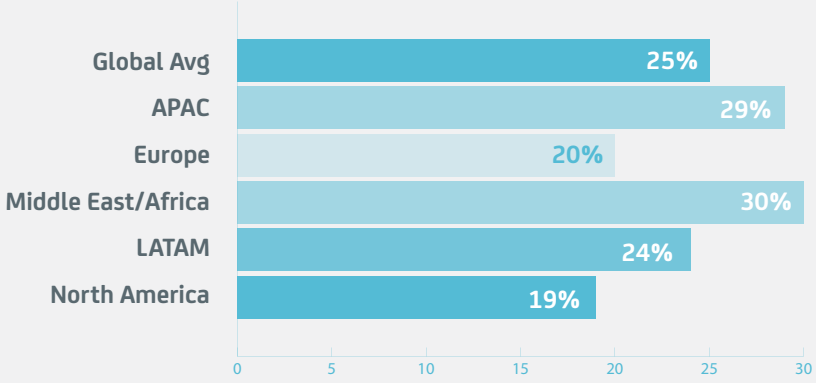
3 Companies must consider the importance of trust. One-fourth (25%) of all respondents were averse to giving personal information freely, with respondents in the Middle East/Africa (30%) and Asia-Pacific (29%) exceeding the global average. (http://www.nielsen.com/us/en/insights/news/2013/-free-and-easy-loyalty-program-benefits-that-matter-most-globally.html)

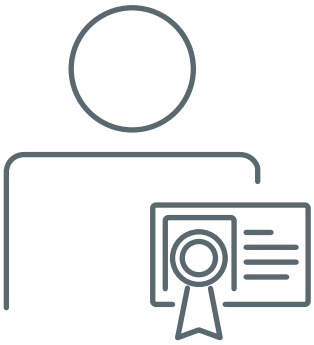
4 Are you likely to shop at a retailer that offers a loyalty program?



Source: Nielsen

5 Percentage of respondents that say not having a strong sense of security would cause them to not join a loyalty program or cause them to opt out.





Regardless of the sector, these surveys demonstrate just how important it is for members' needs to come first. Members demand a simplified experience and trust that their sensitive data is safe from hacking attacks.

A majority of recent breaches involve compromised usernames and passwords. No member should have to worry about whether or not his or her information is at risk. This creates a lack of confidence in the company's brand and drives the member away, decreasing revenue.

Traditional black-box authentication solutions no longer have a place in today's security framework. Companies should look for flexible and scalable solutions that allow full control over the authentication process. Changes to rules should be made in real-time and behavioral models need to learn and adapt quickly.

Furthermore, companies need a robust case management system that will allow analysts or CSRs to research each login attempt, if necessary. The case management system must also be able to prioritize cases for outbound fraud investigation and focus on the highest priority cases, which ultimately reduces the cost of fraud investigations.

Multiple facets must come into play in order for companies to successfully secure members and themselves from loyalty program attacks. Fortunately, simplified convenient methods of risk-appropriate, strong authentication exist today to help add to the level of protection and help end users in the fight against these increasingly sophisticated attacks.

Why CA Technologies?

There should no longer be any uncertainty; a company must offer a reliable and valuable loyalty program if they hope to remain competitive in the marketplace. This means deploying security capabilities that can help you not only keep financial losses to a minimum by securing against breaches, but also maximiziming member loyalty by establishing genuine trust with members. The only way to accomplish such a feat is to demonstrate innovative thinking when it comes to **outsmarting the hackers**.

Three steps to securing loyalty programs:

1. Utilize strong authentication that's proven and offers a wide range of credential types across a range of devices. Must support unbreachable passwords and possess flexible user authentication and provisioning workflows.
2. Employ risk-based assessment that allows full control over the authentication process (white-box philosophy) and uses a rich set of assessment tools, such as device identification, geo-location, device intelligence and user-behavior profiling.
3. Integrate a robust case management and research system with rule editing and performance reporting that allows access to 100 percent of the data immediately.

CA Advanced Authentication provides zero-touch authentication that incorporates both risk-based authentication methods like device identification, geolocation and user behavior profiling, as well as a wide variety of multi-factor, strong authentication credentials. This helps companies achieve flexible, friction-free security for its loyalty program members.

CA Strong Authentication is a versatile multi-factor authentication system that can help you deploy and manage a wide range of authentication methods, from passwords and knowledge-based authentication (KBA) to two-factor software tokens or hardware credentials. It provides the ability to authenticate users with unbreachable passwords that aren't stored anywhere so cannot be stolen by hackers. It also provides out-of-band authentication methods such as SMS, email or voice delivery of one-time passwords (OTP).

CA Risk Authentication is a powerful risk-based, adaptive authentication solution that works in real time to evaluate context, calculate a risk score, recommend actions and provide alerts/case management. It has a flexible set of prebuilt rules to detect risk and an easy-to-use risk management console to adjust parameters or create new rules on the fly. The risk engine examines many factors including device identification, geolocation, IP address and user activity to evaluate risk. The calculated risk score is then fed into your policies to decide whether to authorize the current activity, request step-up authentication and/or send an alert or block the activity. This provides your organization with a transparent layer of protection against identity theft, data breaches and fraud.

A unified security approach must cover all facets of an organization. Leaving just one area exposed can leave your whole organization exposed. CA provides an intelligent authentication solution that includes all of these critical capabilities and can help both enable and protect your business in the new application economy.

ca technologies

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-134865_0615