Deloitte.

Loyalty data security
Are hospitality and travel companies managing the risks of their rewards programs?

Companies that can persuade their customers to share personalized information about their interests, hobbies, and preferences can create a highly valuable and customized experience: the more information they gather, the more they will be able to personalize the travel experience, and the tighter their bond with customers. But if they fail to live up to their custodial responsibility to secure customer information, that bond can be shattered in an instant.

The current status of loyalty data security presents both an opportunity and a threat for hotels and airlines. According to Deloitte's recent *Loyalty Data Security Survey*, when it comes to protecting personal data, customers hold airlines and hotels to a very high standard, and many perceive these standards are not being met. Physical safety is the number-one priority for travelers,[1] and today that priority is being extended to the cyber world.

The opportunity: Achieving customer engagement and deeper differentiation

Rewards programs are an important element of many airline and hotel customer strategies, but simply offering frequent traveler points is no longer enough to drive loyalty[2] and increased share of wallet. To move to the next level, hotels and airlines are investing in their rewards programs, looking for ways to create personalized rewards and highly tailored travel experiences that will build customer engagement and drive repeat business.

These strategies are based on detailed knowledge of consumer preferences and interests. For example, a hotel might automatically provide a yoga enthusiast with a practice mat and pre-set her room's television to a yoga instruction video. Or an airline that knew one of its best customers was a vegetarian with a nut allergy might send him a special snack with a handwritten note explaining the ingredients. The ability to deliver these deeply personal experiences can distinguish a company from its competition and turn its most valuable customers – frequent travelers – into brand ambassadors.

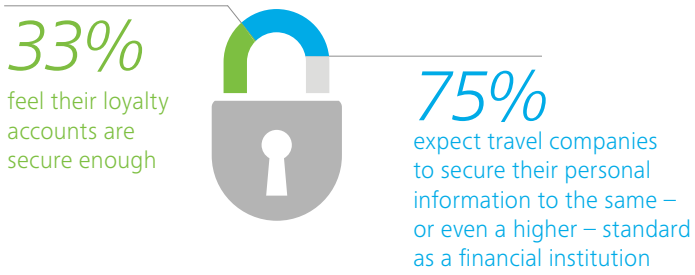
To achieve this level of engagement, travel companies need to know more about their customers; and the only way to do this is by asking consumers to share more potentially sensitive personal information.

The threat: Security risk and reputational damage

Collecting and housing such a broad array of sensitive and personal data exposes travel companies to a heightened level of cyber risk. Much of this information, while subject to a jurisdiction's rules governing privacy, is not given the same protection standards as, for example, credit card numbers. By its very nature, this data is not anonymous, and there is not always a requirement that it be encrypted, making it vulnerable to cyber thieves, disgruntled employees, and others. Furthermore, in order to create a seamless travel experience, travel companies often partner with one another or with third parties and lifestyle brands such as fashion or luxury goods. Most of these initiatives involve sharing customer information via digital channels, allowing data to move outside the company's control and potentially moving it into a less secure environment where a breach might occur.

A breach of loyalty program data has the potential to seriously damage a company's reputation, prompting travelers to shy away from or abandon the brand in the future. Even in the absence of a breach, most consumers don't have sufficient confidence in airlines and hotels to entrust them with the type of personal data they require to deliver truly innovative and customized experiences. In order to persuade customers to share more personal details, travel companies will need to first convince them that their data is in safe hands and then demonstrate there is a reward for sharing.

The disconnect between expectations and perceptions



Expectation vs. perception: A troubling disconnect

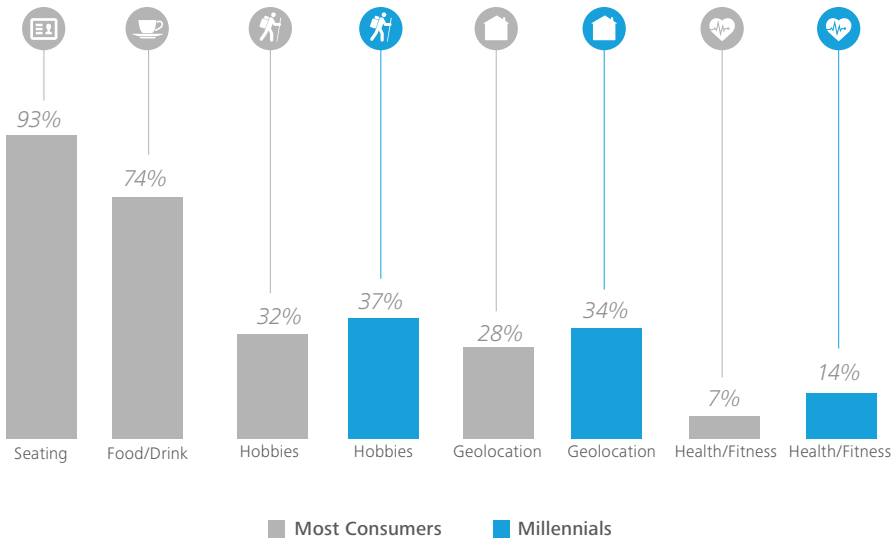
Security of sensitive personal information such as credit card numbers and social security numbers is a top concern for most consumers today. Companies that collect and maintain other personally identifiable information in their systems have a wider duty to protect it. Most consumers don't make a distinction between travel companies and companies in other industries when it comes to this responsibility. In fact, three quarters (75 percent) expect travel companies to secure their personal information to the same – or even a higher – standard as a financial institution. This may be due to the fact that travel companies are going beyond the basics, requesting that their customers share an ever-more detailed level of personal information.

Despite their expectations of travel companies, only a third (33 percent) of travelers feel that their loyalty accounts are secure enough. Although Millennials are slightly more comfortable with security standards, with 40 percent saying they believe their information is secure, the low level of trust among travelers is concerning, and it appears to be restricting the amount and type of information they are willing to share.

Most consumers (93 percent) are willing to share travel preferences such as seating choices, and nearly three quarters (74 percent) are comfortable sharing their food and drink preferences. Yet many draw the line at more personal data such as hobbies (32 percent), geolocation (28 percent), and health and fitness records (7 percent). Millennials are only slightly more comfortable sharing this data: 37 percent will share hobbies, just over a third (34 percent) will share geolocation, and 14 percent are comfortable sharing health and fitness records with loyalty programs.

This reluctance to provide more personal details could limit the degree to which airlines and hotels will be able to truly tailor the customer experience and achieve the level of intimacy that will allow them to "own" their most valuable customers.

What are loyal customers willing to share?

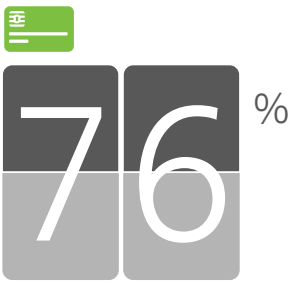


Loyalty data breaches: The potential for a significantly bigger impact

Security breaches have become all too common in recent years, with news of data theft hitting the headlines with disturbing regularity. The majority of travelers (76 percent) are concerned that a loyalty program breach would result in loss of credit card numbers. Fifteen percent are simply concerned that a breach would result in theft of their loyalty points. Clearly very few are aware of the wider risks when private data, including travel schedules and other sensitive personal information is lost, publicly exposed, or used illegally. But the danger is there.

When a breach of loyalty data does take place – and it is only a matter of time before it does – it will serve as a wakeup call for consumers and companies alike. The precedents already exist: Witness the numerous burglaries that have occurred when homeowners enthusiastically post their "away from home" status and adventures to social media sites. Theft of digital travel information could have a similar impact, and could even place people in physical danger should a break-in occur while some family members remained at home. As one survey respondent noted, "My biggest concern is that if there was a breach that they would know where I live and have all my info. Money can be replaced, but my daughter cannot."

A breach of loyalty data would have significant impact on brands. Nearly a quarter of respondents (23 percent) said should such a breach occur, they would be less likely to patronize the company responsible for the loss of their data, and 15 percent said they would be a lot less likely to do so. Given the fact that these frequent travelers are by far the most valuable customer segment for hotels and airlines – and that disgruntled consumers often have an outsized influence on others via social media channels – a data breach has the potential to cause serious reputational damage and revenue loss.

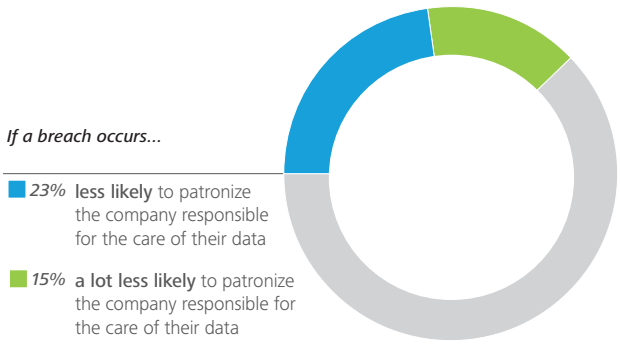


concerned that a loyalty program breach would result in loss of credit card numbers

concerned that a breach would result in theft of their loyalty points

"My biggest concern is that if there was a breach that they would know where I live and have all my info. Money can be replaced, but my daughter cannot."

-Survey respondent



Making the customer part of the solution can lead to brand engagement

With the rapid pace of evolving technology, new apps, and online conveniences, consumers are overwhelmed. Maintaining good security practices has become something of a burden for today's digital consumer. In juggling on-line accounts with social media venues, financial institutions, and myriad e-commerce sites, it is little wonder they suffer from login fatigue. Travelers are no exception, even though the data they share with airlines and hotels may be of a highly personal nature. Only 21 percent change their passwords at least once per quarter, and more than half (53 percent) use the same password for other accounts.

While consumers' relaxed security practices are worrisome, they present an opportunity for hotels and airlines that are looking for ways to forge closer ties with their customer base. Demonstrating this joint commitment to security might include:

- Launching awareness campaigns to keep security top-of-mind with consumers.
- Sending out periodic emails to customers reminding them to change their passwords or security questions or to check their account activity – and including a link to make the action as easy as possible.
- Offering complimentary points for members who regularly change their passwords.
- Offering free or discounted security services such as apps that manage passwords or monitor security, and rewarding customers for using them.
- Rewarding customers who provide their contact information and sign up for security alert services.

Not only do these reminders offer a legitimate touch point, they are an indication that the company takes its duty of care responsibilities seriously. Once customers feel more comfortable that their information is secure, they may be more willing to provide personal details. Companies will then be in a better position to fully deploy the personalization strategies that will uniquely distinguish their brands.

Only 21 percent change their passwords at least once per quarter, and more than half use the same password for other accounts.

Making data security a priority

Engaging customers to improve lax security practices is not enough, however. Airlines and hotels have considerable work to do within their own organizations to not only better protect personal data but to ensure that consumers understand where, how, and with whom their data is being shared – and to monitor for policy violations.

While every company has a privacy policy buried somewhere on its website, and consumers often blindly accept the terms of complex legal agreements, true transparency is rare. Many consumers are certainly uninformed when it comes to understanding the security and privacy policies of airlines and hotels, including those of their loyalty programs. Forty-one percent of frequent travelers confess to having little or no knowledge of these policies. Once again this presents an opportunity for companies to communicate more openly with customers, letting them know of enhancements to privacy and security measures, and explaining how their data will be used and how this will benefit them.

Finally, travel companies should roll up their sleeves and move beyond mere compliance to ensure that customer data is truly secure. Steps to consider include:

- Assess risks across all transaction points (see sidebar) to identify potential weak points in their security practices.
- Establish the capacity to detect patterns of behavior that may indicate compromise of critical assets.
- Ensure data is only accessed on a 'need to know' basis and that it is housed within a secure and encrypted environment
- If a hotel or airline merges loyalty programs with an industry peer or enters into a joint initiative with a third party that requires sharing of customer data, establish a clear understanding of the other entity's data protection practices and monitor those practices to ensure your guests' data is being appropriately curated.

Protecting the traveler and the brand

For any traveler, physical security continues to be a basic expectation. Whether in the air, or in a hotel, consumers expect to be provided a safe environment. This duty of security is now extending from the physical world into the cyber world and travelers are expecting security of their personal information.

For any travel company, personalization, which is the key to differentiation in a sea of consumer choices, requires companies to collect detailed and often sensitive information from customers. Travel companies invest significant dollars in loyalty plans, which historically have offered increased returns. However, continuing to capitalize on that reward will increasingly depend upon first, maximizing the potential of the data gathered and second, appropriately managing the risks of data aggregation and use.

Companies that fail to live up to their custodial responsibilities to protect consumers' information risk serious damage to their brands. On the other hand, those that go the extra mile to secure traveler data – and to engage customers in the process – will be able to claim customer care as a core element of their brand.

Assessing security risks

The following questions can help airlines and hotels consider any gaps in their security measures for protecting personally identifiable customer information:

- Is there a clear definition of the customer data that is collected and for what purpose it will be used?
- Where is this data used in the organization?
- Is the company aware of all international privacy laws and how does it ensure compliance?
- Is there a clear 'need to know' policy that limits who can touch the data?
- Is the data secured and encrypted throughout its life and in all IT systems?
- How does the company identify a breach of data?
- Is there a response plan in place to contain the impact and protect the brand should a breach occur?
- Is there a complete inventory of third parties (e.g., processors, outsourced providers, marketing firms) with which data is shared?
- What will be shared with third parties in the future? Is there a clear requirement of what can and can't be shared outside the organization?

Contacts

Charles Carrington
Partner
Deloitte & Touche LLP
+1 215 405 7845
chcarrington@deloitte.com

Darrin Kelley
Partner, U.S. Travel, Hospitality and Leisure
AERS Advisory Leader
Deloitte & Touche LLP
+1 213 688 5420
darkelley@deloitte.com

Guy Langford
Vice Chairman, U.S. Travel,
Hospitality and Leisure Leader
Deloitte & Touche LLP
+1 212 436 3020
glangford@deloitte.com

[1] *Rising above the Clouds: Charting a course for renewed airline consumer loyalty*, Deloitte Development LLC, 2013.

[2] According to studies by Deloitte, nearly 40 percent of high-frequency travelers are members of four or more frequent flier programs (*Rising above the Clouds: Charting a course for renewed airline consumer loyalty*) and close to 42 percent participate in four or more hotel loyalty programs (*A Restoration in Hotel Loyalty: Developing a blueprint for reinventing loyalty programs*).

About the survey
This online survey was conducted in April 2014 with 1,000 frequent travelers in order to canvas their views on security and privacy practices of frequent traveler plans. Respondents included U.S. citizens, between the ages of 18 and 94 who had either stayed at a hotel for more than 26 days in the past 12 months or flown more than 25,000 miles in the past 12 months. They also had to be a member of at least one hotel or airline loyalty program.

For more information about our survey, visit www.deloitte.com/us/managingrisksrewards