Managing the Risky Business of Loyalty Programs

March 31, 2015
Joe Mont, Compliance Week

Reach into your wallet or purse. Chances are you have at least one customer loyalty card in there. Regardless of which business issued it to you, the arrangements are all pretty similar: You get discounts or rewards for using the card, and the business learns more about you and your buying patterns.

The compliance and privacy consequences of loyalty programs and their data, however … the arrangements around those can be pretty fluid. Amid the ever-increasing focus on data and privacy protection, it may be just a matter of time until regulators take a tougher stand on even the most basic loyalty programs.

The list of risks is long. How such data is stored and protected is ripe for scrutiny, experts warn. Are the terms and conditions customers signed being upheld, or will the Federal Trade Commission swoop in to slap an issuer with a fine for "unfair and deceptive practices"? Loyalty programs can also run afoul of antitrust laws, torpedo a merger, complicate a bankruptcy proceeding, violate the Health Insurance Portability and Accountability Act, and garner unwanted attention from state regulators.

Companies are paying closer attention to perk programs. In 2013, CVS Caremark abandoned plans to bring prescription purchases under its traditional rewards card. Critics, state attorneys general among them, objected to the HIPAA waivers customers were asked to sign. More recently, Toys R Us, American Airlines, and United Airlines all chose to notify customers of loyalty program breaches in recent months.

The changing view of personal data is one reason these programs will come under greater scrutiny. "Their position is that if you collect information from consumers, it is an unfair practice not to keep that information secure," warns Gary Kibel of the law firm Davis & Gilbert. "So, if there were a breach and it was just a name and e-mail address, they could still assert some kind of an action."

Disclosing a loyalty program breach has its own set of concerns. "Typically if you see companies notifying the loss of rewards, it is probably something they elected to do voluntarily and not because they believed that it was required under the law," says Nathan Taylor, a partner in the data security practice at Morrison & Foerster. "But no good deed goes unpunished. You may not have a legal obligation to provide notice, but once you elect to, it is quite possible you will get a resulting regulatory scrutiny or even class-action lawsuits."

When a company looks to sell or share its database of loyalty program information, other concerns arise. Case in point is RadioShack, which sparked a minor outcry when word leaked that the

company wants to sell its massive customer database as part of its bankruptcy proceedings; consumer activists question whether that move violates customer privacy protections. A similar debate has emerged in the bankruptcy proceedings for Caesar's Entertainment. The casino chain values its rewards card program at $1 billion, making the program one of the largest assets Caesar's owns.

"The question of loyalty programs and anticompetitive practices is very much in play and the law is less than fully clear."

Timothy Smith, Founder & Managing Partner, Wiglaf Pricing

"One of the big assets that come up as part of the selloff with the bankruptcy option is personal data that a company has collected over the years," says Christian Habersaat, a partner with the law firm Goulston & Storrs. "That is actually a question that is being looked at by courts and state attorneys general right now. There is opposition to the release or sale of personal data when there are questions as to whether consumers knew, or should have known, that it could be shared with others and under what circumstances."

"When you sign up for those programs, you are not generally anticipating that the information could be transferred to another organization and is an asset a company might someday sell," says Margaret Utterback of the law firm Quarles & Brady. She draws a comparison to Facebook's $22 billion purchase of the messaging service What's App in 2014. The FTC intervened when Facebook first told users it would maintain What's App's existing privacy agreement, and then changed its mind. The FTC could likewise intervene in similar situations involving the sale or transfer of loyalty program data.

Headaches Not Just for Consumers

Corporations also develop incentive programs to reward other companies that are steady and loyal customers. Those deals could set the stage for a violation of antitrust laws.

Some programs have been deemed illegal for issues that have nothing to do with consumer privacy or protection, says Timothy Smith, managing partner of Wiglaf Pricing, a consultant that works with companies to price products and services. "There is an anti-competitive issue here, but only for super-dominant firms with higher than 50 percent market share, reaching toward 90 percent," he explains. "The question of loyalty programs and anti-competitive practices is very much in play and the law is less than fully clear."

CRACKING DOWN ON DATA BROKERS

The following report, with legislative recommendations, was released last year by the Federal Trade Commission. It addresses the use of consumer data by data brokers and is viewed by many data privacy experts as foreshadowing a greater focus on customer loyalty programs as well.

The Commission recommends that Congress consider legislation requiring data brokers to give consumers (1) access to their data and (2) the ability to opt out of having it shared for marketing purposes.

Currently, consumers do not have meaningful information about which data brokers may have their data, nor do consumers have meaningful information about where they can access their data or how they can exercise any opt-out rights that data brokers may already provide. To enable consumers to efficiently avail themselves of these rights, legislation could also require the creation of a centralized mechanism, such as an Internet portal, where data brokers can identify themselves, describe their information collection and use practices, and provide links to access tools and opt outs.This approach would enable consumers to visit a single site to ascertain what kinds of information data brokers have about them and how to exercise opt-out choices.

The Commission recommends that Congress consider requiring data brokers to provide consumers with access to their data, including any sensitive data, at a reasonable level of detail. Because data brokers create and manipulate thousands of data elements and segments, it would be very difficult for consumers to interpret and digest an access tool that gave them access to every category of data a data broker has about them. Despite these challenges, Congress should consider requiring data brokers to provide enough detail that a consumer can see the breadth of categories the data broker has about them, including any sensitive data.

Source: FTC.

In 2009, for example, European regulators hit Intel with a $1.45 billion fine for its customer loyalty program in the silicon chip industry. In 2010 the FTC also investigated those practices, which rewarded buyers who used a high percentage of Intel chips in their products. While Intel was not found to be selling its chips below cost, regulators justified the fine on the grounds that it harmed Intel's competitor, AMD, because Intel held a dominant market share. Intel was required to pay AMD $1.25 billion.

"When it comes to customer loyalty programs that have some form of price discount or rebate, the law seems to say that you are free to do what you want unless you are a Goliath," Smith says.

There are ways companies can minimize the risks that may arise from loyalty programs. Review, at least on an annual basis, the terms of use customers agree to. The program should collect only the data needed to manage a program, nothing more. "There is a concept in the privacy world called data minimization—collect what you need," Kibel says. "You would hope that a supermarket's loyalty card does not somehow contain information about the prescriptions from their pharmacy, or Social Security Numbers, because that would be a poor design."

Databases should be separate and segmented if no reason exists to connect them to other platforms. "If I'm an attacker coming after you, and you glom all your data together, I'm going to have a field day," says Randy Sabett, a privacy lawyer at the law firm Cooley. "If there is one little chink in your armor, I get in, and all your data is just sitting there monolithically, and I am going to get it. If you do the segmentation properly, you have made it much more difficult for a hacker to get at the stuff they want."

The FTC takes the view that if you are doing what you told your customers you would do with their information, take reasonable steps to protect it, and incorporate "privacy by design," there should be few concerns. "But if you have done something you told your customers you weren't going to do, you are going to be in their crosshairs and you will be fined," Utterback says.