

IN THIS  
ISSUE:

7

**Nectar:  
Sweet or Sour?**

8

**Happy Birthday,  
Reward Zone**

10

**The Umbrella Effect:  
Cendant's TripRewards**

# COLLOQUY®

Published by:

FREQUENCY  
MARKETING®

WE DO  
ONE THING  
AND WE  
DO IT WELL™

THE VOICE OF THE LOYALTY MARKETING INDUSTRY SINCE 1990

WWW.COLLOQUY.COM

**COLLOQUY'S  
European Vacation**

*...in which we journey  
across the Big Pond  
and find that loyalty  
marketers in Europe  
have a thing or two  
to teach us jaded  
Americans. Join us  
for the whirlwind tour...*

## You Don't Have to be Paranoid— But It Helps

BY JIM KUSCHILL

LOYALTY PROGRAM REWARDS REPRESENT VALUE TO CONSUMERS. BECAUSE OF THIS VALUE, THERE IS INCENTIVE FOR UNSAVORY SORTS TO COMMIT FRAUD OR TO OTHERWISE TAKE ADVANTAGE OF YOUR COMPANY'S LARGESSE. IN THIS TWO-PART SERIES, TECHNOLOGY EDITOR JIM KUSCHILL IDENTIFIES THE WARNING SIGNS FOR FRAUD AND GIVES YOU THE TOOLS TO DEFEAT IT.

➔ The central problem is this: there are lots of very smart people out there with time on their hands. If enough of them identify your loyalty program as a target, then some of them will achieve a modicum of success. Fraud generally springs from three primary sources: employees, program members and vendors. Groups can also collaborate to commit fraud, and can often be harder to catch than individuals.



Your program design will determine the form that any potential fraud may take. You should conduct a fraud potential analysis during your program planning stage, and consider monitoring for fraud to be a loyalty best practice. To do less is the marketing equivalent of strolling through a dangerous part of town after dark with \$20 bills bulging out of your pockets.

That said, here are a few of the more common types of fraud for which you should be on the lookout:

### **The Secret Swiper**

Perhaps the most common type of employee fraud, the Secret Swiper falls under the category of "good intentions gone awry." Mr. Customer forgets his membership card, and your sales associate kindly offers to swipe his own card— either to give Mr. Customer that point-of-sale (POS) discount, or so the employee can collect a few reward points of his own. Either way, the gambit can play havoc with your customer valuation process.

Fortunately, this fraud is easy to catch by implementing a few simple reports relative to transaction volumes. Simply establish a threshold for transaction counts over time, or perhaps for the transaction size. If any member account exceeds these parameters, then send in your fraud-sniffing dogs.

### **The Double-Dipper**

Most consumer loyalty program rules prohibit employees from participating—often because employees already get a nice employee discount. But many employees join the program anyway, knowing that finding employees in the transaction file is a difficult and often error-prone proposition. These double

dippers enjoy both their regular employee discount and the chance to earn loyalty program rewards.

If you're motivated to prevent double dipping, then the simplest solution is to stop issuing points or rewards on any transaction that shows an employee discount. As the employee discount is typically a more lucrative reward than the points issued, the rule stifles the behavior. If you want your employees to participate, let them know a dozen times in a dozen ways that you look for fraud and when found, the consequences will be very bad.

### **The Paper Pusher**

If your program issues paper certificates, then you open yourself up to a whole host of fraudulent activities. The simplest, and perhaps the most prevalent, type of fraud involves multiple redemptions of a single certificate. These paper-pushers can play havoc with your program return-on-investment (ROI).

The simplest solution here is to implement real-time verification of certificate numbers. If your rules engine or IT infrastructure won't allow for that, then have your employees collect or mark the certificates in such a way as to prevent their reuse. If possible, include certificate numbers in the POS transaction log so that you can track redemptions back at headquarters.

Batch tracking activity can turn up not only fraud, but also simple training issues—maybe your associates are scanning one certificate many times rather than each individual certificate provided by your members. POS coding can prevent this. If that's not in the cards, then find the means to compensate for paper pushing and train your associates accordingly.

### **Whining for Dollars**

Every associate can no doubt tell tales about member complaints. *I never received my certificates in the mail. My mother-in-law stole them. My dog ate them.*

We've heard it all before.

If you can't accurately confirm that a member has or hasn't redeemed her certificates, then you won't have any choice but to re-issue them. You approve the certification redemption without verifying the certificate number, and then *hey presto!*—the member suddenly finds the missing certificates and brings them in to redeem a second time.

These scenarios might represent attempts to defraud, but they could also simply be honest mistakes. Maybe Mr. Customer's mother-in-law really did steal the certificates, and then felt guilty about it. In any event, you need to track the situation on the back end and devise decision-tree responses to various scenarios. In the case of the member cashing in a second set of certificates, allowing an account balance to go negative is a reasonable possibility.

### **The Return Monsters**

Fraud opportunities often arise from the program rules themselves, or from the technology devised to implement the rules. Many of these fraud loopholes revolve around the Returns Department.

The root of the problem is time—the time between when a purchase takes place and when a return occurs. Consider the member who makes a big purchase on the 1<sup>st</sup> of the month. You run your certificate extract on the 15<sup>th</sup> with a mailing just afterward, and the member returns the items on the 25<sup>th</sup>. That member has now obtained certificates for which he isn't eligible, and likely now has a negative point balance. Now what do you do?

Long-time loyal members might simply be going about their business quite oblivious to the situation, in which case you do nothing—their point balances will eventually go positive. If, on the other hand, you see this behavior in new members—or if you see multiple returns in the same account, then you are possibly being scammed.

Loyalty program rules can actually compound this problem. One company had a rule preventing member balances from going negative—if the account went negative, then the point balance was adjusted *up* to zero. Imagine the fraud potential here—it's breathtaking. Fortunately, no mass fraud occurred, but the potential was certainly there. Eliminate the problem by allowing negative balances.

### **The Reverse Spammers**

If you issue certificates via e-mail, then you have real problems. When you send certificates by mail,




you at least have a bona-fide physical address for the account—a place to send the police if things get really bad. If you issue certificates virtually, however, then the e-mail address might lead you anywhere, from the actual member to an empty studio apartment in Manila.

A simple way to mitigate this risk is to require some sort of validation process for the virtual account via a physical address. For example, don't allow electronic coupon distribution until the member confirms the receipt of a PIN or password through the mail.

### **The Bonus Pigs**

Let's say that a member makes a large purchase during a program bonus period, and then returns the items after the bonus period ends. Unless your POS log contains the original purchase date, you can't correctly debit the bonus points from the member's account. Worse, if you issued a soft benefit, such as a tier upgrade, as a result of the purchase, then you can't very well revoke it no matter how smart your POS.

The simplest solution to this problem is to delay posting transactions until after the return period ends. This isn't exactly the most member-friendly solution in this age of instant gratification, and it can therefore have a dampening effect on member enthusiasm. But it does help solve the problem.

As you do your fraud contingency planning, the most important rule to bear in mind is that your fraud controls must be invisible to your members. No one likes to be suspected of fraud, and the quickest way to lose a good customer is to accuse him falsely. In the next issue, we'll look at more tools and tips to help catch the real scammers. 

*Jim Kuschill is COLLOQUY's technology editor. He also recently made quite an impression dancing the Electric Slide at the editor's wedding.*

*"You should conduct a fraud potential analysis during your program planning stage, and consider monitoring for fraud a loyalty best practice. To do less is the marketing equivalent of strolling through a dangerous part of town after dark with \$20 bills bulging out of your pockets."*