



**SPECIAL REPORT: THE 2004 LOYALTY MARKETING SUMMIT**  
**Art and Science of Customer Yield Management**  
Beginning on page 10

IN THIS  
ISSUE:

7

**Life Beyond Credit:  
Private-label Best Practices**

8

**The Kuschill Report:  
Homeland Security**

12

**Special Report:  
The World Coalition Colloquium**

# COLLOQUY®

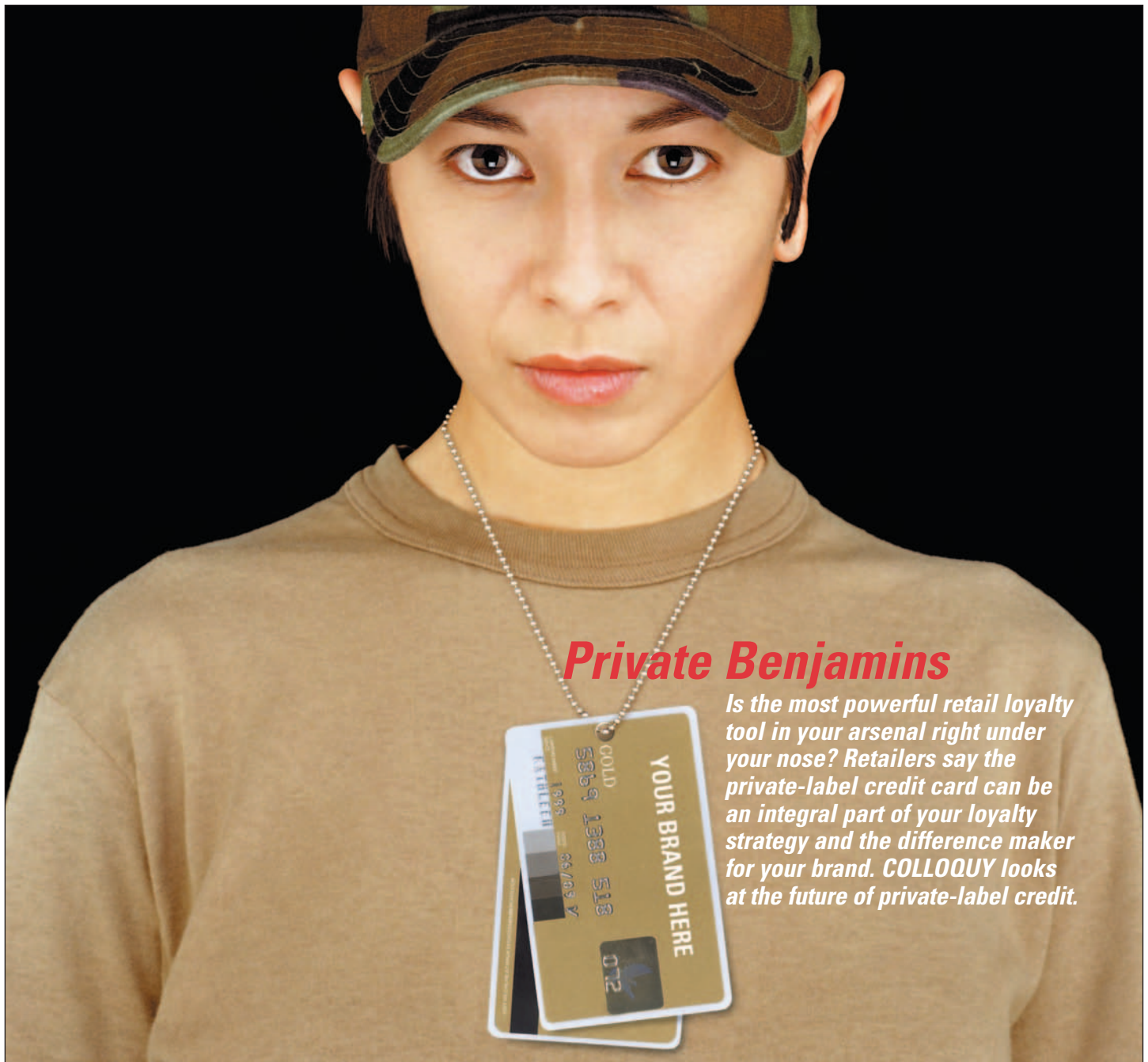
Published by:

FREQUENCY  
MARKETING®

WE DO  
ONE THING  
AND WE  
DO IT WELL™

THE VOICE OF THE LOYALTY MARKETING INDUSTRY SINCE 1990

WWW.COLLOQUY.COM



## **Private Benjamins**

*Is the most powerful retail loyalty tool in your arsenal right under your nose? Retailers say the private-label credit card can be an integral part of your loyalty strategy and the difference maker for your brand. COLLOQUY looks at the future of private-label credit.*

## Homeland Security

PREVENTING LOYALTY FRAUD MEANS NEVER HAVING TO SAY YOU'RE SORRY

BY JIM KUSCHILL

IN PART I OF JIM'S SERIES ON LOYALTY PROGRAM FRAUD, PUBLISHED IN OUR LAST ISSUE, WE LEARNED ABOUT HOW TO SPOT THE VARIOUS SPECIES OF LOYALTY SCAMMERS IN THE CONSUMER WORLD AND TAG THEM BEFORE RELEASING THEM BACK INTO THE WILD. IN PART II, WE LEARN HOW TO SPOT AND ADDRESS FRAUD WITHIN— GASP!— YOUR OWN ENTERPRISE.

➤ Sadly, your own call center and IT departments can be fertile ground for loyalty program fraud. Would that it weren't so, but we've seen it many times. Fortunately, catching fraud in the call center and back office is not an insurmountable task. Here are a few of the more common scams to look for:



### The Insider

The easiest way for a call center representative (CSR) to perpetrate fraud is to simply place an adjustment into an account from which the CSR benefits—the account of a friend or relative, for example. Ideally, you should both limit the size of adjustments your CSRs can make and track both the number and point size of the adjustments. If you need to adjust many point balances a substantial amount, perhaps because of servicing or other issues, an ability to forward an “over limit” adjustment request to a supervisor or manager can work wonders.

### The Parasite

Another favorite CSR ploy: locate an account with a high balance, adjust the member's address and then redeem against the account. Obviously, the victimized member will complain about this, and irreparable harm to the relationship could result. For that reason, it's a good idea to attach employee IDs to member address changes and to review the log on a regular basis.

### The Ship-to Switcharoo

Some programs provide for alternate ship-to addressing for awards, which invites fraud. To plug this leak, consider requiring a password from the member before you allow the CSR to specify an alternate ship-to address.

You might think that it's possible to limit most fraud on member accounts by prohibiting call center access to member accounts without passwords. Unfortunately, from our experience this solution seems to cause more trouble than it's worth. Members forget their passwords; talk times go up; supervisors get involved; member

frustration increases. But requiring a password only for a ship-to change is a less troublesome solution.

### The Points Cartel

Many programs allow members to combine accounts. This makes sense when members marry or if a member has accidentally opened multiple accounts. Unfortunately, this loophole can also leave room for CSRs to combine accounts for their own benefit—a move that effectively bypasses all of the aforementioned auditing on adjustments and addresses. As account combinations should happen infrequently, you could restrict this function to supervisors—and then log all occurrences.

### The Gift Gambit

Some programs allow members to forward currency from one account to another as gifts. Any time you allow the transfer of currency from one account to another, you invite fraud. At a minimum, you should allow only the “from” account to make forwarding requests. Better still, to prevent forwarding to unintended places, require the “to” account to either accept or decline the forward. As with the Ship-to Switcharoo, use of a password before the transfer is allowed is a good idea. Again, maintain and review logs for all account transfers.

### The Under-debit

If your program offers travel awards such as airline tickets or hotel stays, you can be hit by fraud involving up-booking of the award, or alternately, debiting too few points from a member's account. For example, a CSR might book a first-class ticket, but only withdraw points for an economy-class ticket. You can sometimes identify this problem via a software comparison of the booking against the award. While the coding of this function is often complex, the payoff can be great.

At this point, we transition away from the front-line troops to what I like to call the “engine room” people.

These are the IT and operational folks who implement special software routines, make certain that data gets from one point to another, and so on. At this level, assuming basic controls, most attempts at fraud will be fairly sophisticated. Here are a few basic back office controls you should consider implementing:

### **Tag Your Files**

In terms of basic data controls, both inbound and outbound files should include header and trailer records. The header records or file names should include sequence numbers, which ensure that no one slips additional files into the processing stream and that none are missed. The trailer records should include record counts and hash totals—both make it more difficult to insert or delete a record from the file or to change values within the file. Record sequence numbers, counts and hash totals in a secure location.

### **Reconcile Accounts**

Periodically reconcile all account balances. You should, for example, compare last month's overall point balance with this month's point balance, and include points issued, changed and redeemed. Do the same for award inventory numbers and other key numbers to help ensure there isn't any "leakage." Overall, you don't need to track a large number of checkpoints, but you should go deep—you'll need enough detail that, if you uncover a problem, you can quickly identify the root cause.

### **Build Physical Controls**

If you print certificates or fulfill merchandise yourself, you need to put physical audit controls in place, such as preprinted sequential numbering of certificates. Because of the ready availability of color copiers, any certificates should contain watermarks or other items not readily reproduced by anybody in the handling chain—including your members. If you have the means, then deploy real-time verification of redemption eligibility. If you issue gift cards, you should generally not load them until it's time to ship them—and compare the load totals to the requested totals to ensure against any monkey business.

### **Lock Down Your Data**

In addition to logging CSR changes to your database, you should also lock down certain data so you can accurately reconstruct a situation. For example, let's say that you've established a currency bonus in your system for a certain time period. You configure the bonus and members start accruing points. What happens if you later notice that a parameter—say, the



start date—on the bonus is incorrect? If you change the parameter value, you might invalidate your audit trail; move back the start date, and some members who should get the bonus won't, and you won't know why. Logging alone won't correct the problem. Instead, lock down parameters on the bonus that could invalidate the audit trail after you award it.

### **Centralize Control**

Implement a configuration management system, and always deploy software changes from the configuration management database. This helps ensure that you only run approved software. Institute a policy of check-in and promotion of software changes, ideally with some form of code review. This helps ensure that Trojan Horses, trap doors, or other nefarious pieces of code are not allowed into your builds. Disable standard accounts provided within your operating and database management systems. Don't allow the sharing of passwords or accounts. Plenty of books describe how to secure software and systems, and security gets more complicated every day.

You may think to yourself, *I'm only running a little itty-bitty loyalty program. I don't need to worry about this stuff.* Yes, you do. You must worry not only about your loyalty program rules, software, and procedures, but also your firewalls, DMZs, separation of responsibilities, and so on. As far as security goes, you're only as strong as your weakest link—whether you control that link or not. Log, audit, track and control—and you'll sleep soundly, knowing that you've implemented your own version of homeland security. ☺

**Jim Kuschi** is COLLOQUY's technology editor and the chief technology officer for Frequency Marketing, Inc.

*"You may think to yourself, I'm only running a little itty-bitty loyalty program. I don't need to worry about this stuff. Yes, you do. As far as security goes, you're only as strong as your weakest link."*