

IN THIS  
ISSUE:**8****Brand Strategy:  
Loyalty at NASCAR Speeds****10****Technology:  
A World Without Cards****12****Program Spotlight:  
Borders Turns the Page**

# COLLOQUY®

THE ART AND SCIENCE OF BUILDING CUSTOMER VALUE

WWW.COLLOQUY.COM

**SPECIAL REPORT:***Trends in Entertainment and  
Leisure Loyalty Marketing*

## ***The Persistence of Memory***

*With the modern consumer's hectic days resembling Dali's famous melting timepieces, leisure marketers find themselves scrambling to cling to both share of wallet and share of clock. If you can spare a few minutes, join COLLOQUY as we learn how innovative entertainment and leisure marketers leverage the power of their industry to build retention and loyalty—and keep time from running out.*

## A World Without Cards

IN THE POKER GAME KNOWN AS "CREDIT-CARD SECURITY," IS THE BEST HAND THE ONE CONTAINING NO CARDS AT ALL?

BY JIM KUSCHILL

WHILE IT MAY BE HERESY TO OUR FINANCIAL SERVICES READERS, THE ONGOING GAME OF NO-LIMIT POKER BETWEEN CREDIT CARD FRAUDSTERS, MERCHANTS, BANKS AND ISSUERS HAS SOME EXPERTS WONDERING IF IT ISN'T PAST TIME TO MOVE BEYOND WALLETS AND PURSES FULL OF PLASTIC CARDS. CAN FINANCIAL SERVICES MARKETERS LIVE IN A WORLD WITHOUT THESE UBIQUITOUS SLICES OF BRAND EQUITY? COLLOQUY'S TECHNOLOGY EDITOR LOOKS AT THE PAST, PRESENT AND FUTURE OF CREDIT CARD AUTHENTICATION.

➔ Credit card users can now brandish cards glowing with every color of the rainbow (including patented clear cards), emblazoned with any variety of themes or pictures and possessed of a variety of fancy shapes. For those of you that missed it, the Japanese issuer JCB recently released the first *scented card*—scented in citrus, although I'd prefer a chocolate-scented card myself.



Despite these drastic cosmetic changes, the essential function and basic security features of credit cards have evolved relatively little in response to the repeated assaults of identity theft and fraud. The consumer world has changed radically, but credit cards are still trying to catch up with yesterday's consumer. Are issuers simply building better vacuum tubes, when we really need transistors? And is it possible to imagine a world without cards?

### Grading on a curve

To compete in today's marketplace, any payment technology must stand up in three basic functional areas: reliability, flexibility, and security. If we approach the plastic credit card with a blank slate, what sort of poker hands does it hold?

**Reliability:** Of supreme importance to payment technology is its reliability to consumers—does it work every time, flawlessly? The credit card payment infrastructure includes the issuers' systems, which clear a card for use; the network over which the authorization and capture takes place; the merchant's point-of-sale or ecommerce infrastructure; and the card itself.

Authorization has evolved from a couple of people talking over the phone into a fully electronic and virtual network. The system deploys redundant computers and networks within a redundant infrastructure. I can't remember the last time I was

told "the network is down." So we'll give credit cards a straight flush for reliability.

**Flexibility:** For the most part, any individual card offering is not in itself flexible—using multiple cards achieves flexibility by leveraging particular cards based on their specific value propositions, which is why our wallets are so thick. Savvy consumers don't carry cards because they're pretty, have a cool shape, or smell nice, but because of their collective flexibility and value. Overall, flexibility is good. But because the redundancy and that wallet bulge bother me, I give credit cards a so-so pair of jacks for flexibility.

**Security:** I'll grade this last but most important issue straight away—"F"—which I would have done even before my identity was stolen—twice. In poker terms, it's a 2-7 offsuit. Let's examine security basics of identity and authentication to see how the credit card is letting us down.

- **Identity:** Your identity is sacrosanct. In a retail credit transaction, you assert your identity with your physical presence, your credit card and your signature. In an ecommerce environment, you present an identifier, such as a user name and password, as well as your card number and perhaps the card's security code. In either environment, your claim to your identity must be authenticated.
- **Authentication:** The three methods of credit-card authorization are producing something *you have*, such as a credit card or security fob; something *you know*, such as a password, a PIN or the answer to a secret question; and something *you are*, such as a match with your photo ID and

your signature. Poorly secured systems depend on only one of these methods, while highly secured systems depend on all three—perhaps with repetition (e.g., *two* items you know). Visa's Payment Card Industry (PCI) standard, designed to protect online data, requires "two-factor identification"—typically an encryption fob ("something you have") and a PIN ("something you know").

How does the credit card stack up against these three methods of authentication? First, I don't need a physical credit card ("something you have") to use it. "Card not present" transactions are a matter of course in ecommerce, catalog shopping, and in other phone transactions such as ordering pizza. Usually I am asked for the CVV2, the three- or four-digit code that—because it appears on the physical card and presumably can't be obtained by dumpster-diving—helps prove that I have my card and that I am me.

Second, credit card authentication systems typically don't require "something you know." Last but not least, card issuers have toyed with biometrics technology, which employs fingerprints, voiceprints, or even keyboarding cadence to improve "something you are" identification. But the jury is out on the usability of a technology that can be expensive to deploy, is in many cases easily fooled, and often fails with false positives, false negatives, or both.

Certainly in a retail environment, requiring a physical card and a PIN provides two-factor identification, and in debit transactions this system works well. But as more transactions move to "card not present" channels, the security bandages—whether EMV-related or not—become useless. Add the growing plagues of computer screen-scrapers, keyboard monitors and malware infections, and it's clear we're heading toward a huge problem.

### **The credit card sunset**

In this current toxic climate, can the ubiquitous credit card survive? What options might yet save the credit card?

**Consumer control:** What if we made added security protections voluntary? Might these additional authentication steps themselves represent a value proposition component? After all, my homeowner's insurance premium goes down if I install a burglar alarm. What if my interest rate were lower, my rebate higher, or my points-per-dollar doubled if I "subscribe" to a higher level of security and reduce the fraud risk assumed by issuers and merchants?

**Virtual accounts:** In the online world, perhaps we could return to the early days of ecommerce transactions facilitated by virtual credit card account numbers, or VANs. You use a VAN (provided by your bank) in lieu

## **How the cards were dealt:**


*In this timeline of credit-card innovation, we see the industry introducing incremental steps to stop the crooks, and we see the crooks taking incremental steps to overcome industry controls. Not included in the timeline are introduction dates for cards featuring cosmetic innovation like shape, color and smell—though perhaps a foul-smelling card might work as well to deter theft.*

|                   |   |
|-------------------|---|
| <b>1920s</b>      | Company-issued cards (essentially the first private-label cards) made available |
| <b>Circa 1938</b> | Companies begin accepting cards from other companies                            |
| <b>1946</b>       | Charge-It (first bank-issued card) introduced                                   |
| <b>1950</b>       | Diners Club creates its classic card  |
| <b>1958</b>       | American Express, Bank of America issue cards resembling modern credit cards    |
| <b>Early '70s</b> | Magnetic stripes are introduced   |
| <b>Early '80s</b> | Holograms are introduced  |
| <b>1993</b>       | CVV (card verification value) introduced  |
| <b>Mid '90s</b>   | EMV standard released   |
| <b>2005</b>       | CVV2 introduced   |

of your real account number, safeguarding the real number against malware detection. However, the typical channel for getting a VAN is the internet—which leaves us in a Catch-22. Still, the idea may be worth revisiting.

**New security channels:** New, more secure channels for authentication might yet save the day. Reference the recent PayPal Mobile announcement of a service that allows you to pay for items via text messaging. You message PayPal, which provides the funds *after* calling you back for confirmation. Another service, TextPayMe, offers similar capability. Indeed, the cell phone presents an intriguing option. What if you could place "self-authorization" controls on your credit card? If a charge exceeds your pre-set limits or falls outside your designated geographic region, the issuer calls you for confirmation.

If such authentication models gain consumer acceptance, why do we need a physical card? My account number would exist only in my phone. I could apply as much added security to those accounts as I desired. If I wanted, my PIN could be  $\pi$  to the 20<sup>th</sup> decimal place. I could back up all this information in some undisclosed secure location just like Dick Cheney—a USB flash drive stored in my safety deposit box would work. Within a few years, your credit card will evolve beyond the physical to become a mere identifier.

What does this evolution mean to card marketers and co-branders who depend on keeping that little plastic piece of the brand in your wallet? It means that simply coating it with a citrus scent may not be enough. I'd gladly trade the odor for a wallet that doesn't bulge. 

**Jim Kuschi** is COLLOQUY's technology editor and a marketing technology consultant for Perfectly Targeted. Email him at [jekusch@earthlink.net](mailto:jekusch@earthlink.net).

*"Might these additional authentication steps themselves represent a value proposition component? After all, my homeowner's insurance premium goes down if I install a burglar alarm. What if my interest rate were lower, my rebate higher or my points-per-dollar doubled if I 'subscribe' to a higher level of security and reduce the fraud risk assumed by issuers and merchants?"*