



Bell Bottoms And Virtual Cards

by [Steve Brown](#)

Fashion aficionados might find it interesting to know that bell-bottom pants originated with mid-19th century Naval uniforms. The idea was to have pants that flared out at the bottom so sailors could quickly remove their boots in an emergency. Flash forward to the 1960s and 1970s and the fashion becomes all the rage in civilian ranks. Back then, bell-bottom pants were worn by hippies and the rich and famous alike. Remembering photos of Woodstock, the pants are unfortunately not great to wear on rainy days, so the trend eventually faded just as other fashion fads have over the course of time. Nonetheless, older fads can make a comeback every so often. In fact, just this year several prominent fashion designers re-introduced "flares" to the public, hoping to reignite this fashion flame and bring customers into stores.

For bankers, you might be thinking about what sort of cards these customers will carry. Several years back, a number of credit card issuers provided consumers with virtual credit card numbers. The numbers on these cards are generated randomly and can only be used for a set amount of time. These one-time use numbers are designed to give consumers peace of mind when using online vendors in that fraudsters who might intercept the number won't be able to use it for long.

In theory it sounds great, but in practice the virtual cards never caught on all that well with consumers for a variety of reasons. For one thing, no one really knew they were widely available. For another, customers that were game to experiment found the process unwieldy - so much so that many decided the extra time spent outweighed the potential benefits. Today there are very few banks that promote virtual cards and two large card brands, Discover and American Express, no longer even offer the option.

We wonder, however, whether we're on the cusp of a new trend. It's been widely reported that online fraud is expected to surge in the wake of the industry switchover to EMV cards this year. This was true in other countries in the wake of EMV adoption. In the UK, online fraud climbed 79% in the first three years after the country switched to chip cards, according to a report by the research firm Aite Group. This won't necessarily indicate an overall increase in fraud. Counterfeit cards will be much more difficult to produce and therefore fraud is likely to move from card present to card not present. The use of PINs would offer vastly better security in that PINs are hard to steal and easy to change, but most card issuers think a PIN will discourage customer card use and therefore won't require one.

At present, Bank of America and Citibank continue to offer virtual cards to consumers for making online purchases. In early June, US Bank announced it had updated its mobile corporate payments

app with features that allow the use of virtual card accounts. Users can now request virtual card accounts and have them delivered right to their mobile devices to make payments. Maybe this represents a better technological advance.

It will be interesting to see whether other banks start promoting virtual cards as well. It hasn't happened to a large extent so far, even with the rash of card-related security breaches affecting a number of well-known merchants. But we may reach a tipping point, depending on the degree to which online fraud continues to rear its ugly head.

Even if virtual cards don't create as big a splash as bell-bottoms, it's highly likely that bank customers will start to demand products that offer better protection from cyber thieves. Some of these products may even mean additional revenue for banks that get the pricing structure right. Maybe it is time to give some thought to future possibilities, as you dust off those old polyester relics hanging in the back of your closet.

BANK NEWS

M&A Activity

1) PayPal has agreed to buy digital money transfer provider Xoom for \$890mm in cash. Xoom allows people to bypass banks and transfer money digitally to 33 countries. 2) Post Oak Bank (\$916mm, TX) will acquire Security State Bank (\$157mm, TX) for an undisclosed sum.

Opportunity

Crains reports that as of yesterday, Chase will no longer take loose change and will require it to be wrapped by customers for deposit. Further, the report says Chase staffers also said coin counting machines are too expensive to maintain, create onerous lobby lines and get in the way of providing customer services, so they won't be provided either.

Idiot Show

The PM of Greece has pushed the country to the brink of disaster, as The Wall Street Journal reports the banking system there only has about \$1B in cash left (will run out shortly).

Regulatory Action

The CFPB has ordered two credit card add-on vendors that provide identity theft and credit monitoring services (Affinion Group Holdings and Intersections Inc.), to pay about \$10mm to settle allegations of charging customers for services not rendered.

Rate Hikes

JPMorgan projects Q2 GDP will climb to 2.5% vs. 2.0% estimated prior, as increased construction activity provides additional support to the economy. JPM predicts 2 rate hikes are likely in 2015 (Sep + Dec).

Risk Concerns

A Bank Director survey of bank executives and board members on risk finds 82% say cybersecurity is the category of risk that concerns them most, followed by compliance (52%), credit (37%) and operational (35%).

Risky Situation

Fed Governor Powell said in a speech that banks "will be attacked" by criminals, so implementing preventative tools and defensive tactics is needed if the bank is going to "survive the game." He also warned bankers that a study has found more than 20% of security incidents are attributable to

insiders, so segregation of duties, background checks and monitoring for anomalies are all part of strong risk management programs.

Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.