A Consultant's View

Vol. XXI No. 6 June 2014

Digital Loyalty

We were recently asked if we had a "Digital Loyalty" program. What the sales people want is a program that slides into a merchant's setup without any additional hardware or cost. There isn't a digital loyalty program that fully meets that want. Nearly any effort to get a digital program will require hardware at the merchant site and might require multiple Apps. Right now, targeting only part of the market might be enough.

In a recent Transaction World, Harold Montgomery asked what he thought would be the perfect mobile wallet. No existing mobile wallet came even close to what he wanted. However, his vision suggests ways to get there.

Customers Have Many ID Methods

Part of his vision is unattainable: "no expensive POS equipment to break down". That is impossible as payment or loyalty is a three way transaction. It is a transaction between the customer, the merchant, and the payment or loyalty system. That requires that the merchant have something that interacts with what ever the customer is carrying. Merchants will need some kind of equipment.

That is where the problem for digital loyalty occurs. There isn't one piece of equipment that will interact with all the different ways customers present identification. Customers are carrying cards, simple mobile phones, Android phones (some of which support NFC), and iPhones. Who knows what customers will carry in just a year or two. For a merchant to handle even some of these, we are talking about multiple ways. We may need an NFC reader for some, we may need a 2D bar code reader for others, or we may need a Bluetooth device. There isn't one simple way to interact with what customers are carrying.

The proposed hardware has a wide range of costs. A bar code reader that can read a QR code from a phone screen is a lot more expensive than a Bluetooth reader. Yet few counter top credit card devices will read either. In most cases, we are faced with having to put hardware at the merchant site.

If we decide to not cover the whole market but target a portion of the market, we can put together a digital loyalty program that covers that specific market (just like a mobile wallet can be designed for a specific market). We can target those who are carrying iPhones and recent Android phones and plan on providing NFC and Bluetooth readers to the merchants. We can provide the POS software and the mobile Apps for those devices. However, trying to get a system that will cover all cases is very large undertaking because the base line infrastructure just isn't there yet.

To make matters even more complicated, it would be nice to be able to interact with the customer where the customer is. That means interacting with the customers on Facebook, Google +, and anywhere else they might be looking.

The only thing that we can rely on is that customers will be changing what they do year by year and we need to constantly revamp what we do in order to meet them where they are.

Digital loyalty is not a sure thing.

EMV – the risks

Although Visa has mandated that merchants either switch to EMV or accept the liability, the risks of moving to EMV have not been widely known. EMV is not the panacea that some people are stating. The reality is that it is also pushing some liability to the card holder.

EMV is supposed to make it impossible to present a stolen credit card number to a merchant and have it be accepted. Unfortunately, there are still ways that criminals can get around the limitations and use stolen cards for value. Merchants can break EMV and defraud both the bank and the cardholder. A recent article in the Communications of the ACM listed a number of ways that have been used in the field by criminals to break EMV. According to a presentation by the Minneapolis Federal Reserve, the president of PayPal had his EMV card ripped off.

Cardholders are assuming more of the risk. A major problem is that people think that EMV is secure. In the case of merchant fraud, the assumption in any transaction in question is not that the merchant is at fault, but the cardholder is. The cardholder winds up being defrauded and not the banks. One report from Britain suggested that one in five of such defrauded cardholders did not get their money back.

One way to break EMV is to insert a skimmer into the card reader and capture both the card and the PIN. That information can then be used at an ATM to clean out the account.

Since it will take years to completely convert the US market, we will see more inventive ways to break EMV. It is important to train customer service about what merchant fraud looks like in order to keep the cardholder secure.

A Consultant's View is published by Prairie Trail Software, Inc.,

Making *Information* from Streams of Data

1-800-618-4199

www.prairietrail.com

Risky World

P.F.Changs is coping with a major data breach by reverting to manual card imprinters and dial up verification. It is a reminder that we all need to keep back up systems for when disasters happen and we go for weeks without power.

Prairie Trail Software, Inc

3821 Beaumont Lane
Plano, TX 75023

Address Service Requested

Prairie Trail Software, Inc.

Making *Information* from Streams of Data

Custom Gift and Loyalty Solutions

For the Retail and Restaurant Trade

We provide technology for

Merchant Services

We pull the whole system together
- or just the parts you need

Custom Gift and Loyalty Card Servers

Database Design and Management

Web Services and Portals

Servers and Dialup Software

Terminal Software

Custom solutions to meet your needs

Call 1800-618-4199
www.prairietrail.com