THE STRAWHECKER GROUP
The Trusted Advisor To The Payments Industry

# A TSG Roundtable on the Target Breach, EMV and the Ramifications

*2/05/14*

***Featuring The TSG Team, including Kurt Strawhecker, Jamie Savant, Gerritt Kerkstra, Linda Perry, Chuck Fillinger, Cliff Gray, and John Kirkpatrick***

## 1) Given the growing number of very public and large merchant Data Breaches, is EMV the answer?

- It is logically true that card data will be safer with a full implementation of EMV at the point-of-sale, removing personal data from the decade old technology of the mag-stripe certainly makes sense.
- However this solution has shortcomings as well, such as Card Not Present (CNP) transactions which will be unaffected by this technology change, which today accounts for 8% of U.S. card payments. Potentially under EMV, fraud will be directed to CNP transactions – and consumers may feel misled by the inevitable continuing data breach stories.
- There are also major operational and technology related issues to solve – such as implementation in restaurants where the transaction still primarily takes place at the table (where's the PIN pad?).
- Mobile commerce may also become a target just as it is about to gain traction in the marketplace.
- Unfortunately, EMV is comparatively old technology, but it would provide a global standard that would ease consumer card use from country to country.
- We're still sorting out if debit cards will have to accommodate aspects of the Durbin Amendment (such as two or four networks) with a common AID or multiple AIDs. That's certainly one of the issues slowing down the issuance of debit EMV cards.
- It will be important to make sure the public does not see the implementation of EMV as a panacea – because it is not.
- The key issue is to get all the stakeholders in the Payments Industry (the Brands, Bank Issuers, Acquirers, Processors and Merchants) to cooperate to fund and implement this major change.

## 2) What is the current cost of fraud?

- Six basis points of fraud or $2.040 billion in the U.S., which is essentially 6 cents for every $100 of electronic payments spent. (Est. $3.4 trillion total V/MC volume * 0.0006 = $2.040 billion)
- At the time EMV was introduced in other non-U.S. markets, fraud losses were generally higher on a percentage basis than what issuers have deemed tolerable in the U.S. As more markets move to EMV, the U.S. is now the lone standout.
- It is important to remember that the U.S. is the largest storehouse of data today so criminals come here to get it and to use cards. It's partly a matter of volume and opportunity.

## 3) Who pays for fraud?

- Half of fraud costs get borne by issuers, and they have been one the hardest to convince to move to EMV and the Brands don't really want to hand out bigger checks. The other half of fraud is borne by the acquirers.

- Obviously, fraud is not distributed evenly across all merchants, it occurs in pockets. Most merchants get away clean - they can't imagine it ever happening to them – making the investment required by some merchants harder to accept.

## 4) Is more government regulation the answer?

- The politics of the EMV issue have changed dramatically since the Target and subsequent retailer breaches. When this arcane technology issue becomes the subject of a USA Today editorial, as well as other mainstream media stories – along with the public's demand to 'fix the problem', a legislative approach is not out of the question. Several large processors, acquirers and the Brands have reported getting calls from their congressmen demanding to know what is being done to solve the issue.
- The Payments Industry needs to understand – data breaches have become a major issue in the minds of consumers. The Target breach, as well as other well-known retail breaches, have created anxiety, with many consumers believing their personal information has been exposed – sometimes due to erroneous news reports.
- Banks may have contributed to the sense of alarm when major national banks made the unprecedented decision to limit ATM withdrawal limits to $250 and debit purchases to $1000 in the wake of the Target breach. This may have had the unintended effect of implying the consumer's cards had been breached. When in reality, issuers may have been trying to stem their potential liability. Some issuers appear to be inconveniencing their cardholders rather than issuing EMV cards more broadly. Now however, we are likely to see much greater EMV issuance in the U.S. as the liability deadline approaches.
- Medium and Large Merchants have begun to see the light after the data breaches affecting their partner companies. Acquirers are reporting a sudden uptick in calls on how to implement EMV and token technology into their operations. This is a pleasant surprise given merchant resistance to date on investing in new POS technology and hardware. Small merchants however will likely continue to lag in converting given the somewhat non-existent ROI.
- At the end of the day will EMV be mandated by Congress? Probably not, only because Congress has a lot on its plate today. Meanwhile the Electronic Transaction Association (ETA) is proposing a standardization of Data Breach Notification laws as a Federal statute to replace the inefficient and overlapping 40+ individual state laws that govern how a merchant must notify its customers of a data breach – that is legislation we can all believe in. This legislation is gaining quick traction even this week in Congress.

## 5) EMV is old, but it does work for all Card Present Transactions (CP).

- Not all data breaches occur at large retailers - two of the largest data compromises occurred at acquirer processors (Heartland Payment Systems and Global Payments).
- The other large data compromises have been at big merchants with masses of information that they protect to varying degrees.
- As noted earlier, fraud may migrate to CNP. CNP has always provided a security challenge and fraud always flows to the weakest link.

## 6) Where does the money come from to pay for EMV?

- Unlike earlier payment industry major innovations – such as the move to electronic transactions, major pricing incentives were used. In this case, brand incentives do not appear to be in the mix.
- It may be a tough sell to the merchant, but Target, Neiman Marcus and Michael's Stores may be thinking differently now. In fact, Target announced in their appearance in front of a Congressional subcommittee on January 4, that they are fast-tracking a $100 million smart card program. Target's chief financial officer, John Mulligan, announced, "Since the breach, we are accelerating our own $100 million investment to put chip-enabled technology in place. Our goal: implement this technology in our stores and on our proprietary REDcards by early 2015, more than six months ahead of our previous plan".
- Again, all elements of the payments ecosystem will share in the cost (some more equally than others).

## 7) It appears none of the parties involved – the card Brands, the issuing banks, the acquirers, or the merchants are incented to implement EMV.

- While there may not be interchange incentives for EMV, there are other incentives, including reduced PCI scope costs incurred on an annual basis, and a reduction in Account Data Compromise fines and issuer recoveries once a significant percentage of a merchant's transactions qualify as EMV.
- To the Brands, PIN traditionally meant lower interchange to merchants and Interlink. Their move to EMV is based on signature and Visa and they say there is no need for PIN. They aren't giving this up anytime soon due to the huge signature base of cards, even with Durbin.
- Many credit card issuers don't care for PIN. PIN on credit signal losses due to cash advance and then bankruptcy. That is why the industry has resisted pushing cardholders to get PINs on credit - plus PIN meant lower interchange to merchants.
- To the Merchants, they see EMV as yet another electronic payments expense after paying too high swipe fees – (even after Durbin).
- Most acquirers see EMV as a messy and potentially expensive implementation that may be similar to Y2K – with the hundreds of end points, VARs, IVRs and POS hardware that will need to be mitigated in a very short period of time. However, as with many mandated programs, some acquirers will find a way to profit from the implementation.

## 8) The current Visa/MasterCard settlement class action suit (unique to the U.S.) has altered the landscape

- If the banks had less money in the partnership deals, the Brands might incent in other ways as they used to, but times have changed. i.e., interchange reduction to merchants was a loss to issuers.

## 9) Thoughts on regulation

- The big issue is - do we want or need regulation in the industry whether at the bank, Brand, or merchant level? We do not believe that government can solve this complicated issue with more regulation.

- We have confidence in the answer is better working relationships between the Brands, banks acquirers and merchants. Perhaps it is in the PCI Council or maybe a new forum is the answer.
- One potential consequence of the breach events is that credit usage may see an uptick as consumers begin to more fully understand the inherent fraud protection credit provides vs. debit. This would be in contrast to the debit usage increases seen since the recession.

### So where are we?

- Due in part to the Target breach, we expect the Brands will reinforce the current EMV schedule and dates.
- Visa Inc. chief executive Charles Scharf on Thursday (January 30) reinforced that EMV is proceeding as planned, "In 2011, we had announced a plan to migrate the U.S. to EMV technology through a liability shift beginning in October 2015 and we have reaffirmed these dates," he said in a conference call with analysts.
- Chris McWilton, President of MasterCard U.S. while not directly reinforcing the announced dates said "it is time for EMV in the U. S." in an article in the NYT recently. There was also a recent report on CBS News with Tim Murphy of MasterCard.
- At the end of the day, the political pressure (Government and the consumer) is too great to resist at least a partial solution to the growing data breach issue.

## About TSG

The Strawhecker Group (TSG) is a management consulting company focused on the payments industry. The company specializes in providing financial institutions, merchant acquirers, card associations, ISOs, processing companies, large merchants, and the investment community with advisory services to maximize their growth and profitability. TSG is also a resource of merchant acquiring industry research, benchmark studies and developing trends. For more information please visit http://www.TheStrawGroup.com.

## Contact Us

402.964.2617
Info@TheStrawGroup.com