

LAISSEZ-FAIRE?

Do We Need Government Intervention at All?

By Jim Romeo

"Laissez-faire" is the French expression for "let do" – meaning keep the state out of trade and let the market forces themselves govern.

This isn't entirely the case with the electronic transactions industry, although the industry is attempting to regulate itself through the card associations.

At the end of September 2007, the deadline loomed for those handling credit cards to adhere to PCI compliance. The PCI DSS version 1.1 guideline officially went into effect, requiring that all credit and debit card handlers adhere to a stricter set of data protection rules implemented by the PCI Security Standards Council — which is backed by prominent card issuers including AMEX, MasterCard and Visa.

Visa USA says that about half of their merchants are Level 1 merchants with transactions of six million or greater. As of the past summer, about 45% were compliant while a greater percentage had plans in place to become compliant soon. It may take weeks or months to see how the end of September deadline affected the industry.

"The Payment Card Industry Data Security Standard (PCI DSS) has been an effective standard since its inception more than two and a half years ago," says Michael Petitti, Chief Marketing Officer at Trustwave. "As a result, thousands of businesses and organizations are more secure and able to conduct e-commerce without exposing consumer information. The standard has been developed by the industry with experience from both processing and security experts. As a result, the standard has generated significant attention and widespread adoption."

A study was commissioned by security solutions provider RSA corporation and conducted by Forrester Consulting. The research is entitled "The State of PCI Compliance."

The study surveyed over 600 market players and came up with some interesting information. The survey reached out to Level 1 merchants or those processing more than six million transactions (for a single card brand) per year and Level 2 merchants, or those processing one million to six million transactions per year. Also, just below the Level 2 merchants are the Pre-Level 2 or those processing 750,000 to 999,999 transactions per year.

The survey found that 72% of Level 1 merchants said PCI compliance was a "very high priority," while only 45% of Pre-Level 2 merchants defined protection initiatives in the same way. According to the study, more than half of the merchants surveyed plan on spending between two and four percent of their 2008 IT budgets on credit card data protection — an increase from 2007 budgets.

The study further points out the following:

For merchants with higher transaction volumes, credit card data protection is a high priority, and risk mitigation is their primary driver. When asked about the current drivers for complying specifically with PCI, 49 percent said they wanted to mitigate the risk of a data security breach. Forty-three percent replied citing pressure from credit card companies as the top driver, followed by potential fines (37 percent), pressure from management (34 percent), pressure from acquiring banks (33 percent), the desire for "best practices" (23 percent) and pressure from customers and clients (20 percent).

The majority of merchants—81 percent—do choose to store credit card numbers, while another 73 percent store credit card expiration dates. Further, many companies also continue to retain information that they are absolutely prohibited from storing:

- 71 percent are storing credit card verification codes.
- 57 percent store customer data on credit cards' magnetic strips.
- The largest providers are the ones retaining credit card data.
- 97 percent of the Level 1 respondents and 80 percent of the Level 2 respondents retain credit card numbers.
- 89 percent of Level 1 respondents retain credit card expiration dates, and 72 percent retain credit card verification codes versus 71 percent and 74 percent respectively of Level 2 respondents.

"The card associations first focused on the merchants who have the most to lose," says Paul Rassori, Vice President of Global Marketing for the San Jose, California- based Verifone Corporation.

Some are critical of PCI compliance. However, it just may be a necessary means to an end.

"While some (mostly merchants) have raised the concerns that PCI DSS is 'too onerous,' many security experts have stood to defend PCI guidance as 'common sense,' basic security," says Anton Chuvakin's, Chief Logging Evangelist at LogLogic. "Indeed, for people living in the security 'stone age,' PCI sounds like a lot, while in reality there is nothing that best-in-class organizations are not already doing. So, stop complaining, get out of the stone age [and] into the 20th century."

While PCI Compliance may work well, it hasn't stopped state legislatures from developing bills that could impose regulations on the electronic transaction supply chain.

When asked about his feelings regarding government oversight from federal or state authorities, Rassori feels government intervention is impending.

"It's inevitable," he says. "No sweeping legislation may be on the federal horizon, but the state of California recently voted on a bill (AB 779) proposed by Assemblyman Dave Jones, D-Sacramento, that places liability on the merchant. Today the penalty that a merchant pays are fines levied by the card associations. This [new bill] allows civil suits to open up [against merchants]." Rassori feels that it is unfortunate that merchants are held to this. He points out that a merchant really doesn't want your private information, but instead your transaction and your business.

The bill was ultimately vetoed by Governor Schwarzenegger saying the card industry had established protocols in place for data storage and security measures.

"This issue and the data security requirements found in this bill will drive up the costs of compliance, particularly for small businesses," Schwarzenegger added.

Rassori says that the card transaction industry has to think how they can assist merchants so this isn't a problem going forward.

Interchange has been one category of fees that legislators have looked at in the past. In fact, the summer of 2007 brought judicial review to evaluate whether or not the big card issuers held a dominant position in the card market and violated antitrust laws. Not everyone thinks getting a judicial review and government regulation are such a good idea.

"I'm not sure a judicial review is prudent, but that doesn't mean it won't happen," says Henry Helgeson, President of Merchant Warehouse. "The landscape of the payments industry has changed in the past few years and card issuers are very aware of merchant dissatisfaction. If card issuers are pro active and open a dialogue with merchants they can still hopefully avoid a potentially damaging situation."

Some merchants are trying to divert transactions to other vehicles other than to the major cards. Recently, in Massachusetts, a supermarket chain was working on developing its own debit card that would allow the merchant to debit directly from the customer's account, saving fees for the grocer who already operates on razor thin margins. This helps abate the fees that are eating up profits on small purchases.

Is this a trend in the making and a possible way to avert interchange fees?

"While the direct debit cards will no doubt find a foothold among certain specialty retailers, we do not see it as being a significant threat to traditional credit card/debit card transactions," says Bryan Ansley, CEO of FNB based in Brentwood, Tennessee. "While it is very desirable for supermarkets and other low margin, high volume retailers to save every basis point they can on each transaction, it is much harder to convince the consumer why they should carry and use these cards on a regular basis. As with loyalty cards, the main reason consumers would use these cards was if there was some

significant cost savings involved for them. Unfortunately, giving the consumer a 1% discount so that the store can save 1.5% on credit card processing fees is not very compelling.”

Henry Helgeson is not fond of these arrangements either. “While these firms provide some savings to the merchant, there still is not a lot of value there for the individual consumers to use alternative payments,” he adds. “These firms will need to find a way to give the consumers more value than current issuers are providing. Until they can provide that value, they will find it difficult to sway consumers to using their systems.”

Finding alternate ways to avoid the long supply chain with high fees from the big card issuers is a result of the expense of a transaction being high relative to the transaction itself. Interchange fees always strike a raw nerve with members of the House and Senate and they don’t take well when the terms and conditions of card fees are not made especially clear to the consumer. Government regulation is always a debatable topic. Some view it as a menace to a free market economy. Others view it as a necessary policing to ensure a free and fair market for all.

“It would be unfortunate if any government body did attempt to regulate merchant fees and interchange,” says Henry Helgeson. “The government would essentially be deciding which benefits cardholders would be able to receive. My worse fear would be an attempt to regulate interchange, or, for that matter, any piece of the acquiring system on a state level. Having to comply with 50 different sets of regulations could prove to be a nightmare for ISOs and processors that conduct business nationally or over a broad geographic area.”

PCI compliance, if it works, may be a successful model of self regulation where an industry can regulate itself and at the same time serve the needs of an entire community of card users at large.

Says Brian Ansley of FNB Merchants, “I like the NFL model with a commissioner versus government intervention.”