DRF Quarterly Spring 2013

Chip and PIN: The Coming Tsunami of Costs for CNP

EMV or what is commonly referred to as “Chip and PIN,” has been adopted by the major card networks as the technology standard to reduce counterfeit and lost or stolen card transactions. EMV has been adopted in most all global markets by issuers and acquirers. What many US merchants don’t realize – especially Card Not Present (CNP) merchants – is the gathering storm of costs this technology will bring as it is implemented in the United States.

We spoke with Dr. Thomas Layman, who helped us understand the forces that will come into play with US Chip and PIN adoption. Tom is the President of Global Vision Group, an international consulting firm in electronic payments and former Chief Economist at Visa.

DRF: What should payment professionals be worried about?

Tom Layman: One of the biggest challenges facing US payment professionals is the use of Chip and PIN technology by the rest of the world. We are caught in a catch 22 situation in that, if we don't adopt Chip and PIN in the US, we'll face increased fraud from criminals who will exploit our magnetic stripe system as other countries systems become more secure. Because it is harder to commit fraud with Chip and PIN, those dedicated to committing fraud will always find the weakest link in the payment system and increasely that is the US since we are one of the last countries in the world to adopt this system. On the other hand, adopting Chip and PIN will lead to hard choices for CNP merchants - choices that will drive up costs and potentially impact online conversions.

DRF: Why will Chip and PIN drive up costs for CNP merchants?

Tom Layman: When Chip and PIN was introduced in the UK, there was a decrease in lost and stolen card rates at the point of sale and ATMs because it became very difficult to create counterfeit cards. At the same time, there was a marked increase in CNP fraud and cross border fraud. Criminals are not going to give up committing fraud because we make it harder; rather they will migrate to the easiest course.

According to the UK Cards Association, face-to-face fraud at UK merchants fell by nearly 70% after the widespread introduction of EMV at the point of sale in 2004. During this same period, however, the CNP fraud rate rose by 50% and now represents 62% of all fraud in the UK. Similar experiences have been noted in other countries including France, Australia and more recently Canada. (Layman)

Every merchant is going to see an increase in costs associated with changing business processes and technology in the transition over to Chip and PIN. How much they lose to fraud is going to be a function of what strategy they chose to follow in the process.

DRF: How is Chip and PIN different from the system we have in the US?

Tom Layman: Chip and PIN was developed initially because in many countries it was difficult to get access to a phone line. Merchants relied on those old knuckle busters and did everything on paper. Phone lines were hard to come by and expensive because in these countries phone systems were monopolies. The chip in the card allowed for a secure, offline authorization and authentication.

In the US, the information to process the transaction is stored on a magnetic stripe on the back of the card and is typically transmitted and authorized by the card issuer or their processor in real time. A card with a magnetic stripe can be copied to create a clone of a card. In contrast, a card with a microchip in it is very hard to duplicate with all the embedded encryption technology. This makes it difficult but not impossible to copy a card. In most environments the magnetic stripe is still fairly secure, especially with the numerical security code on the back of the card, which is unique to the card. The chip does make the physical card more secure, as evidenced by the decrease in face-to-face POS fraud, in every country where is has been adopted.

DRF: Why was Chip and PIN deployed in Europe first?

Tom Layman: Credit card fraud rates were higher in some European countries than in the US. In 2004, fraud in the UK stood at .14 percent per transaction value compared to an estimated .05 percent per transaction value in the US. (King, 2012). The economics were not there to justify making the investment in the US to replace all the POS terminals and ATMs. Now as fraud in the US is approaching .13 percent, according to research by the Federal Reserve, there is increased pressure to change over to a more secure system using Chip and PIN technology (King, 2012).

DRF: What is driving the adoption of Chip and PIN?

Tom Layman: Fundamentally, the challenge of adopting any new technology is related to the mix of costs and benefits of adoption. One of those tradeoffs is where the liability for fraud resides. The issuers and the card networks want to see the US shift to a Chip and PIN system to reduce fraud. The large investment on the part of merchants to change their terminals is requiring the networks to provide both carrots and sticks to encourage the upgrades of the merchants point of sale systems.

One merchant incentive includes the elimination of the requirement for annual PCI compliance validation if 75% of a merchant's transactions originate from chip-enabled terminals after October 1, 2012. For the largest merchants, savings from an annual PCI compliance validation would average approximately $225,000 a year. Further, Visa set October 1, 2015 as the US date when a card-present counterfeit fraud liability shifts from issuers to merchant acquirers, if fraud occurs in a transaction that could have been prevented with a chip-enabled payment terminal. While the announcement lays a path towards EMV chip card migration, it does not necessarily set a path to Chip and PIN as Visa will continue to support both signature and PIN cardholder verification methods (King, 2012).

DRF: What should CNP merchants do to prepare for more fraud?

Tom Layman: Visa and MasterCard have developed 3D Secure to help CNP merchants address growing online fraud. The decline in CNP fraud on UK-issued cards has primarily been due to the growth in the use of 3D Secure by both merchants and cardholders. The challenge for US merchants is that 3D Secure is going to make ordering more cumbersome for consumers. Merchants are concerned that these extra hurdles will lead to more lost sales as consumers drop-off in the order process.

DRF: Are there other technologies CNP merchants might consider?

Tom Layman: There are some companies trying to develop technologies such as Acculynk, which is a software solution, and Anywhere Commerce (formerly Home ATM), which involves hardware. Anywhere Commerce uses USB drives to enable transactions at home that would emulate a Chip and PIN terminal, and their challenge has been consumer adoption. A few companies are looking at dynamic codes produced by the merchant and verified using software on the consumer's side. Also, there is a rumor that Apple is developing a biometric reader for the next iPhone. Initiatives like these could make CNP transactions more secure but the concern is to the extent they will be adding transaction burdens on consumers. A system that requires an additional device or password could result in lost sales. In the meantime, it will be a balancing act for merchants to decide whether or not to use the secure transaction technology and deal with their acquirer when transactions are fraudulent, or, use the technology and lose sales to competitors who are willing to take the risk and potential losses.

The history of Chip and PIN adoption in other countries indicates significant costs are in store for CNP merchants. The challenge for these merchants is to decide what strategy will yield the best outcome when balancing the cost of fraud with the need to serve their customers.