PSCU

PERSPECTIVES

Enough is Enough: Everyone Must Chip in to Prevent Card Fraud

October 2015

For the last decade, the entire payments industry has seen a substantial increase in fraud losses.

In addition to high-profile security breaches at major retailers, the incidence of skimming to steal card information at swipe locations and then cloning magnetic stripe cards to use at retailers has also increased.

While the new EMV technology being imbedded in credit and debit cards will no doubt have a significant positive impact on fraud at the point of sale, it is not a magic bullet. Unlike the magnetic strip on the back of the card that cannot be updated with purchase information, the EMV chip keeps track of each transaction and transmits information to the reader for processing. Whereas the traditional magnetic stripe cards were relatively easy to copy, this two-way communication makes EMV cards much more difficult to clone. However, in order to truly mitigate payment card fraud, all players in the payment processing cycle – issuers, merchants, processors and card brands – must now come together if EMV technology is going to reach its full potential.

Dean Young
SVP Industry Engagement, PSCU

Dean Young leads PSCU's strategic direction on how to best leverage the cooperative's scale to advocate on behalf of the credit union industry. He works collaboratively with key national industry partners to ensure there is alignment on hot topics and a cohesive voice.

Prior to this role, Dean led PSCU's client relationship team, which serves the CUSO's 800+ Member-Owner Credit Unions across the country, for nearly 10 years.

While credit unions, banks, payment processors and card issuers have been working diligently and spending hundreds of millions of dollars to have this new secure EMV technology in the hands of consumers before the recently elapsed liability shift deadline, the merchant community has lagged in its EMV preparations despite having the same amount of time to update their payment acceptance and processing technology. The deadline was intended to motivate merchants to adopt EMV. However, a large

percentage of retailers, especially smaller chains or independent stores, have resisted the change because of the significant upfront cost and the disruption to their operations.

Many retailers have either not yet replaced their credit card terminals or have not enabled the new EMV features. If consumers use their new EMV credit cards in the old terminals, the merchant will now bear the cost for any fraud that occurs as a result. An even greater concern is that fraudsters will target stores without EMV-enabled terminals since they can use their tried and true method of skimming. Upgrading and enabling these terminals is critical. Without it, little will be done in terms of reducing card present fraud and identifying theft.

Job Involves Everyone in Payments Loop

PSCU has been issuing EMV cards to its credit union Member-Owners for more than four years, starting with Andrews FCU in 2011. Our EMV deployment strategy reached well beyond simply ordering chip cards and implementing chip card programs. We conducted numerous EMV educational forums across the country to prepare credit unions for the EMV shift, as well as arming our credit union members with best practices for encouraging member adoption and usage. To date, PSCU member credit unions have issued 2.8-million EMV-enabled credit cards. More than half of all PSCU credit unions have issued EMV credit cards to their members and several hundred more are at some point in the process. And more than 200 are in the process of converting to EMV debit cards.

Using new technology to prevent fraud requires complete participation from all parties in the payments loop. If there are any gaps in the process, you can bet that criminals will focus all their attention and capitalize on those gaps until they are closed. New and emerging authentication techniques such as tokenization, biometrics and other forms of encryption represent the next frontier in payment card security and will add even more strength in the fight against fraud. But the payments ecosystem will not maximize the potential of EMV fraud mitigation technology or any other emerging technologies until all participants are equally engaged.

Perhaps, just maybe, the recent cry from merchants for more time to implement EMV terminals is more about lowering interchange costs – which mandating a PIN would likely accomplish – and less about cybersecurity and consumer protection. Rather than spending their time lobbying the government to mandate PIN transactions, which cost merchants less than signature transactions, their time and resources would be better spent making necessary updates to payment acceptance and processing technology. Enough is enough: the time is now to come together and focus on industry cooperation to beat the fraudsters at their own game.