Renaissance
ASSOCIATES

EMV Is Just Part of the Security Cost for Small Businesses

By Kevin Beasley March 29, 2016

By the time you finish reading this sentence, two more Americans will have fallen prey to credit card fraud.

That's right: according to recent **research**, $16 billion was stolen from 12.7 million U.S. consumers in 2014, equating to one new fraud victim every two seconds. Because of the prevalence of fraud, EMV chip cards have been introduced in the United States as a safer payment option.

These new EMV cards, whose chips are designed to prevent thieves from duplicating cards, are steadily rolling out to consumers from major financial institutions. The transition to EMV-compliant payment terminals on the merchant side, however, has been far more gradual. Although EMV card readers are required by credit card companies under contract, small and mid-sized businesses have been slow to upgrade their systems. In fact, in October, 2015 it was estimated that only 40% of U.S. small businesses have made the transition to the new EMV-friendly point of sale (POS) terminals.

In order to better understand the EMV rollout and its effect on small and mid-sized businesses, it's important to consider three key factors.

Small and Mid-Sized Business Have Been Slow to Upgrade Their Systems. Small and mid-sized businesses have been slow to adopt EMV technology for two main reasons: cost and a limited availability of the new terminals. Although EMV-compatible stand-alone terminals start at around $200 per unit, small businesses in particular are often unwilling to pay for even a few new terminals while their current systems continue to operate. It's much easier to justify allocating those resources to business decisions that have more immediate, tangible effects.

And while that inclination is understandable because small and mid-sized businesses tend to worry less about security threats, it would be wise to remember what happened to a big name retailer in 2013; even a few hundred dollars' worth of new, secure equipment could prevent much larger financial repercussions.

The second reason that small and mid-market businesses have been slow to adopt EMV terminals is the backlog in available POS systems. For many mid-market businesses that are interested in adopting the new technology, their purchases were delayed or prevented due to extended waiting periods by EMV terminal vendors. Companies that waited past the October 1, 2015 adoption deadline are now unable to upgrade their systems in a timely manner because most manufacturers have not caught up yet – even for small businesses that only need a few units, the waiting list is often quite long. Only about 20-30 percent of merchants made the shift by the October deadline, which is far less than what was originally predicted.

Overcoming EMV Adoption Barriers. Financial institutions continue to rollout EMV chip cards to consumers; as they do, they have the opportunity to explain the added security they offer.

This added awareness will lead consumers to recognize and ask if a merchant's payment terminal is EMV compliant and if it is not, they will soon start asking why. Merchants, no matter how large or small, will have to keep up with this demand from an increasingly educated customer base, which will likely lead to a rise in the supply of the POS units. In addition, if compliance begins to be enforced, EMV adoption should increase dramatically as merchants attempt to avoid greater fees. That being said, there is no governing body for EMV, it's simply a shift in liability from financial institutions and card issuers to the merchant if a data breach were to happen at a store, or the bank if they have not issued an EMV card.

The Future of Card Security. EMV adoption has been slow through the latter part of 2015 into 2016, particularly with small and mid-sized businesses; however, the technology offers greater payment security for card present transactions. Even so, because EMV does not protect against online transactions, otherwise known as card not present (CNP) transactions, online fraud is expected to rise drastically. In fact, after the European liability shift, some countries card-not-present fraud increased by a staggering 79%. By making it more difficult for criminals to hack into payment terminals to steal customer information, hackers will funnel their energies toward online fraud just as they did in the Europe. Merchants must be prepared to combat this new wave of crime and financial institutions will need to find new ways to protect their customers online.

Although EMV chip technology improves the security of card-present transactions, there are still several adoption obstacles small and mid-sized businesses must overcome, specifically in terms of cost and limited equipment availability. Merchants must purchase new EMV terminals to protect both themselves and their customers, and vendors must be able to meet this demand. Once the EMV rollout is complete, merchants must find a way to protect their ecommerce transactions as well by transitioning to gateway tokenization.