American Marketer

Business at its best

COLUMNS

Does Target's breach spell threat or opportunity for mPOS?

April 28, 2014

Ken Paull is CEO of ROAM

By Ken Paull

The recent high-profile security breaches involving point of sale (POS) systems in the retail sector did not involve mobile POS (mPOS), but no one in the broader electronic payments industry wants to see breaches happen. We need to work together to eliminate breaches and ensure continued trust in electronic payments.

The only positive from incidents such as the Target breach is that they tend to raise awareness of risks, and an industry that is more aware is one that will be better prepared. We see this heightened interest in security happening now, not just with traditional POS systems, network security and credit card technology, but also in regards to stronger security for mPOS. All in all, that is a good thing.

Changing the conversation
For the past couple of years, mPOS has garnered attention for its ability to help businesses of all sizes, from small merchants to major retailers, drive more sales and bring greater efficiencies to many of their most important customer service processes.

In this early adoption curve, the focus has tended to be on what is cool and different who can offer the sleekest-looking reader, or who can offer a visually appealing payment app. But now any headline regarding breaches is changing the conversation, putting more attention on security.

Resellers and merchants alike are placing a higher value on security and raising the bar above the standards, which have been lagging in the mPOS sector.

In the long run, more attention on security will force all providers to up their games and help reduce security risks. In the short term, however, the market needs to gain a better understanding of what a more advanced level of mPOS security entails.

Layered security
When it comes to security of any type of system, a layered approach is best, and mPOS is different in this regard.

Encrypted card readers is one layer, security at the app level is another, and a third layer includes making sure that as credit card companies and retailers migrate to EMV, the mPOS solution is EMV ready.

As most everyone has probably heard in the wake of the recent data breach stories, EMV cards, used already in Europe and other parts of the world, are more secure than the magstripe technology used in the U.S. market.

While it will take time for the U.S. market to completely move to EMV because of the change-out of infrastructure and the related costs involved, businesses are quickly realizing that it is a necessary step and are starting to plan their the related costs involved, businesses are quickly realizing that it is a necessary step and are starting to plan their EMV migration well ahead of the October 2015 deadline.

There is also a middle tier for mPOS security that tends to get overlooked, but actually can provide some of the most effective security features.

At the heart of this middle tier of security is a "mobile payments engine" that provides the underlying technology powering these mPOS solutions. The most advanced engines can even enable businesses to implement pre-processing controls and set up custom risk profiles.

Raising the bar
The more mature fixed POS market has offered these advanced types of security features for some time and, fortunately, the mPOS market is finally catching up.

As mPOS solutions start to move upmarket to larger retailers and services organizations, chief information officers and other leaders in these companies are simply going to demand a higher level of security out of an mPOS platform.

At the same time, the smaller merchant category where mPOS enjoyed much of its early traction is going to get a nice trickle-down benefit from the trend toward more advanced, layered security features which have demanded by these larger enterprises.

To the casual observer or consumer, mPOS might not seem very secure, since the transactions take place on a device that could be anyone's smartphone. That is because the average consumer does not realize the working of an encrypted reader, or the multiple security layers that make mPOS safe.

Additionally, the nature of mPOS carries some inherent security advantages.

For example, a mobile device is not hardwired into an in-store network, meaning there is no single point or fixed communications line for hackers to exploit in order to penetrate these devices or the data on the network.

When you can combine these inherently secure characteristics with a comprehensive set of safeguards in a mobile commerce platform, mPOS emerges as a secure technology choice in which everyone can have a high level of confidence.

WITH THE RECENT high-profile security breaches in the retail industry, and growing adoption of mPOS among larger retailers and businesses, the bar has been raised on mPOS security features.

Those in the mPOS ecosystem need to do more than just address this threat. They should also be looking at this as an opportunity to lower security risks for solution providers, resellers, merchants and consumers alike.

Ken Paull is CEO of ROAM, Boston. Reach him at kpaull@roamdata.com.

American Marketer is published each business day. Thank you for reading us. Your feedback is welcome.