



BOB CARR is chairman and CEO of Heartland Payment Systems. You can reach him at bob.carr@e-hps.com.

Good, Bad News: Enhanced Security on Way

In my last article, I talked about some of the reasons why the move to TDES is critical for operators with certain types of equipment. These changes will close gaping holes that had been created in the past by some equipment manufacturers.

In this article, we look forward at what is likely to happen in the world of c-store payments, both inside the store and at the pumps. It would be unfortunate for c-store operators to purchase equipment that will not accommodate the anticipated changes likely coming within the next few years.

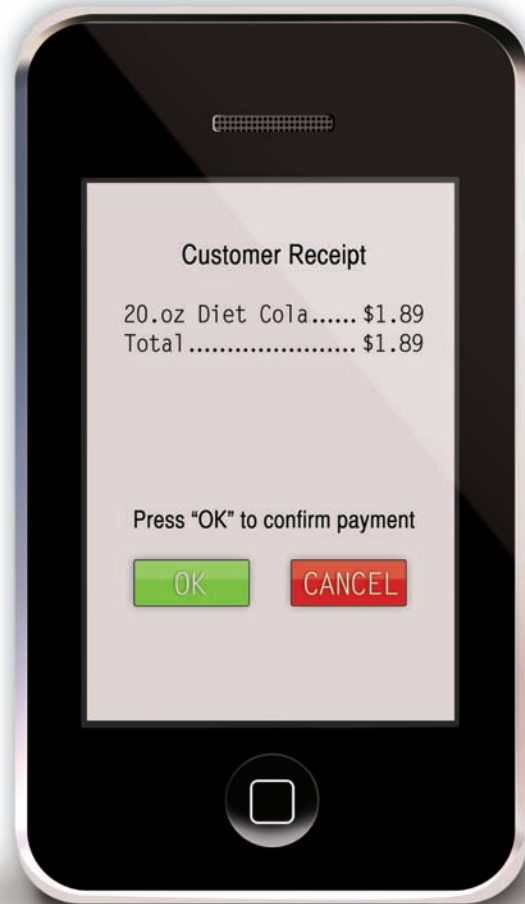
The industry is filled with discussions of PCI compliance, various theories of next steps about what should happen in the future, and who should do what and why. I believe the future is clearer than many would like to believe. A wave is coming—a big one—and it is as inevitable as the tsunami that inevitably follows an earthquake under the ocean.

That wave is the younger generation. They are going to take over the world, and they are going to do it with smart phones year after year. Will this happen next year? No, but it will begin to happen in another 12 to 18 months, in my view, and become more and more predominant as time marches on.

One (mostly unintended) consequence of this is a fundamental change in the landscape of security in the payments world. The good news is that we are finally going to have truly powerful authentication of the consumer, combined with encryption on the front end of the transaction and tokenization on the back end. The bad news is we are going to have to spend money on equipment to read the smart phones and accept the resulting contactless EMV transactions.

A POTENT COMBINATION

There's more good news, though: The scope of PCI compliance will be significantly reduced because front-end encryption means sensitive card data will never enter the system of the operator. And back-end tokenization means sensitive card data can be maintained behind the systems of the merchant's processor. If the merchant never, ever has



possession of a clear-text card number, will the PCI requirement even apply to the payments systems of the merchant?

With dynamic data authentication that is a byproduct of contactless EMV, counterfeit cards will become much less of a problem than they are today. This will significantly reduce losses that currently are absorbed by petroleum retailers due to fraud.

There never will be a silver bullet. However, the combination of dynamic data authentication (a cornerstone attribute of contactless EMV technology); encrypted transactions from the point of entry into the c-store's network; and tokenization of all stored data for settlement and exception processing

forms the holy grail of modern security technology.

In late May, the Secure POS Vendor Association published the first set of requirements ever for enhanced security systems that can be adopted by brick-and-mortar merchants. These requirements apply to inside and outside payment transactions for c-store operators. The industry has been calling for a standard. Well, here is the first attempt. My view is it is a very good start, and industry associations should get behind this initial effort at defining a standard for enhanced security in U.S. payments.

WHY THE CONFIDENCE?

So why am I so confident in predicting what is about to happen over the next few years in a world with so much complexity and seemingly so many alternatives? Here are the reasons.

1. As convenience operators know better than anyone, it's all about the consumer experience. Tapping the cell phone at the point of sale is a more friendly experience than pulling out a card, mostly because the cell phone is within easy reach and doesn't have to leave the consumers' possession.

2. Tapping the cell phone to make the payment allows the consumer to receive instant confirmation of the purchase along with the balance in his account (an optimal security measure in and of itself) plus a coupon or advertisement from the store operator.

3. On college campuses, young people are making e-mail obsolete in favor of social media. Students don't carry cash and often leave their wallet in their rooms. They almost never leave their cell phones in their rooms, and they know 10 times faster if they have lost their cell phones than if they have lost their student ID cards. Twenty years ago, these same students were the first to start flocking to ATMs while the older generation stood in lines at bank branches to cash a check. Eventually, almost everyone started to go to ATMs, and every bank and credit union in America was forced to offer them. This younger generation will lead the wave to contactless EMV, and the older generations will follow again.

4. Smart phones are the ideal instrument to communicate to customers—from making offers and tracking loyalty points to networking and social media. It is an unintended

consequence of smart phones that they will also serve as the most secure payment form on the planet.

5. As with PINs on debit cards, the risk of payments fraud will go back to the consumer with contactless EMV payments authenticated with a PIN. Finally, the risk of accepting electronic payments will come off the backs of the merchant community and be placed firmly on the consumer—just like with cash and PIN debit.

6. We already have seen a plethora of card-reading devices connect to a port in the smart phone. These “sleds” are inexpensive and allow the consumer to swipe each of her cards in her purse and store them in her phone as encrypted information. She can select which payment account she wishes to use for a particular purchase and tap her phone to make it happen. These transactions qualify as card-present transactions because the card is physically swiped when it is entered into the payments chain.

7. The telecom carriers “get it” and are in front of this wave. They decide what kinds of phones the handset manufacturers will build and, as time marches on, a higher and higher percentage of cell phones will be enabled with contactless EMV capability. The estate of cell phones turns over every two years, so advances on the consumer end of this wave will be quick to arrive.

A wave is coming—a big one—and it is as inevitable as the tsunami that inevitably follows an earthquake under the ocean.

phones will be enabled with contactless EMV capability. The estate of cell phones turns over every two years, so advances on the consumer end of this wave will be quick to arrive.

WHAT IT MEANS FOR RETAILERS

So what does this mean for the store operator who wants to keep up with this wave? The answer is simple: Do not upgrade to any new equipment that does not contemplate contactless EMV in the future. Equipment is being built today that can be upgraded in the field to enable contactless EMV at reasonably low cost. Walmart is vocal about its current capability to upgrade all of its stores to EMV today without changing out POS equipment.

Notice this prediction does not mention the card brands or the PCI Council, Congress, trade associations or any of the other parties involved in recent controversies. This is all about the consumer experience and how to better serve the consumer. C-store operators are the best at managing the consumer experience. It will be delightful to watch the ingenuity and creativity that will be upon us before we realize it. Smart phones are going to change our world! ■