How EMV Compliance is Enhancing Self-Service Bill Payment

Enhance Customer Experience Through Self-Service Bill Payment

MERIDIAN
CONCEPT TO COMPLETION

How EMV Compliance is Enhancing Self-Service Bill Payment

Enhance Customer Experience Through Self-Service Bill Payment

Businesses are turning to bill payment kiosks to enhance customer experience through self-service payment. Bill pay kiosks offer customers a secure transactional solution and provide businesses with a new way to improve customer service. Kiosks are mostly unattended devices, providing self-service solutions across a wide range of industries and use cases. With the rolling implementation of EMV "chip and signature" and "chip and pin" cards in the U.S., improved security for consumers and decreased fraud for merchants are compelling benefits for bill payment kiosks.

Beginning on October 1, 2015, the U.S. took the first of several meaningful steps in joining the rest of the world in fighting credit card fraud as the EMV system took effect. With this step comes a shift in liability related to counterfeit transactions. EMV is the acronym for Europay / MasterCard / Visa, the three organizations that developed the specs, and is the global standard for cards with computer chips and the technology used to authenticate chip card transactions.

Think of EMV as a "front-line of defense" that protects against the use of stolen or counterfeit cards at retail point of sale (POS). Under the new system, if a retailer accepts a chip card but doesn't have a chip reader, the card issuer will no longer bear responsibility for fraud if the card is counterfeit, shifting the burden to the retailer. If both the card issuer and retailer have adopted EMV chip card technology, the liability remains with the issuer.

There are exceptions to the October 2015 shift: ATMs and automated fuel dispensers will not completely participate in this liability shift until October 2017. The new EMV liability shift also does not apply to "card not present" transactions (mail/internet/phone orders).

However, EMV does not prevent data breaches and hacks into back-end POS systems. The goal of EMV is to make it impossible for someone to use a stolen or cloned card. Security breaches and hacks seem to be in the news all the time, raising consumer awareness of the need for improved security and protecting their information. To merchants, EMV is about managing the high cost of fraud and maintaining consumer trust.

The liability shift is a compelling event for large retailers, who have significant revenues and customer bases and can afford the high costs of the new POS terminals and integration processes. They have a better chance of a ROI from EMV than small retailers. The implications for retailers are significant in terms of costs and managing fraud. New POS terminals are required to accept chip cards, and the costs are significant in terms of the terminals and integration into retail POS systems.

Cost estimates from the NRF and other retail industry groups range up to $35 billion. But fraud is a huge problem and costs $8.6 billion in the U.S. annually according to the NRF, and the new EMV chip cards have the potential to drive that way down based on experience in the UK and Canada. In Canada, fraud due to debit card skimming has dropped by almost 80% since 2009 according to Interac, Canada's leading payment system.

What does this mean for kiosk providers and buyers?

The first issue is that kiosks are usually unattended devices, delivering self-service solutions. This means that the kiosks can't use a basic POS terminal – an OEM approved for unattended use is needed. They have a higher degree of security in them that prevents people from getting in and accessing the keys to the data.

A major point about EMV is there are three pillars to become a solution that is certified. If any one of the devices changes, it's required to be recertified with the EMV managing and certifying organization called EMVCo.

The three pillars are:

- Certified hardware/payment terminal: lots of these exist
- In combination with #1 is certified software
- In combination with #1 and #2 is a certified merchant bank

Level 1 EMV compliance relates to the hardware, and Level 2 relates to the software driving the hardware. There are tradeoffs. Transactions happen between the POS device directly with the bank. Current kiosk vendors will have to adjust to that because they are accustomed to handling a customer's personally identifiable information (PII). But the problem with handling PII is a significant PCI compliance issue with security and liability risks.

For kiosk vendors the EMV system means a limited set of hardware options. For example, a Level 2 certified solution, can include the following highlights:

- Certified unattended hardware including indoor and outdoor
- Certified commercial off the shelf (COTS) software with an EMV/PCI certified stack
- Deliver additional certified technology and offer a single point of integration with the COTS software as well as other devices like cash and check and scanners.

EMV compliance can be complicated and costly, and marks a milestone with the Liability Shift in the U.S. But card issuers need to complete chip card distribution, and more merchants need to participate, before the U.S. can see the positive impact on fraud that the rest of the world has seen.

"Retailers found it an expensive transition to EMV, however now that the transition is complete, all maintenance costs are just a routine cost of doing business. It's now rare to find a retailer that does not use EMV in Canada. Consumers are expecting retailers to have EMV terminals now, and are skeptical if they do not.

— Paul Burden,
Director of Software, Meridian

Questions to Ask Before Investing in a Bill Pay Kiosk

What problem are you trying to solve?

The first consideration of a payment kiosk should be the use case. What will the kiosk be used for? While this may seem like a simple question, there are many different types of payment a kiosk can support. For example, more traditional use cases include tuition collection, rent payment and bill collection. However, advances in self-service technology now allow kiosks to dispense tickets, print documents and encode cards to meet the demands of multiple industries.

How do you plan on conducting sales?

How a business plans to conduct sales in a self-service environment is a key factor in determining the best bill pay solution. It's important to know what the expectations of the customer will be. For example, is the expectation that a customer will scan and purchase a physical item? Is the kiosk being used to sell a service, pay for a bill, or will the kiosks be used to expand the shelves by selling more products than a business can carry in store?

Who's creating the user interface and maintaining the platform?

The kiosk software platform and application will determine the user interface and how customers engage with a bill pay kiosk. A comprehensive bill pay software solution should provide businesses with custom reports, system performance management, system security, a wide range of component support and configure with all major credit/debit cards.

What are the physical requirements?

The use case, business model, security and software determine which devices and components are needed for the bill pay kiosk to succeed. Comprehensive software will allow component integration from a large inventory of devices. Device and component integration can include a printer, card encoder, dispenser, scanner, VoIP and more.

mzeropay | MERIDIAN CONCEPT TO COMPLETION

Corporate Headquarters
312 S. Pine Street, Aberdeen, NC 28315 | +1 866-454-6757 | sales@mzero.com

meridiankiosks.com