Bankcard fraud costs the United States card payment industry about 8.6 billion dollars each year.

Although there have been some large retail establishments profiled in the news, small businesses are also at risk. Recent surveys indicate about half of small business have experienced a security breach or even multiple breaches.

The good news is that by moving to EMV standards and Chip Based Smart Cards, it is estimated that losses from lost and stolen bankcards will reduce by about 95 percent.

In this lesson we will review the benefits of using EMV and some related terms. We will explore the concepts of Authentication and Verification, Contact and Contactless. The system requirements to use EMV will be also be addressed.

The acronym EMV stands for Europay, [pause] MasterCard, [pause] and Visa.

The EMV Company was formed to help facilitate global compatibility of chip-based payment cards and acceptance devices.

EMV does this by using authentication technology when the card is presented to ensure that the card is real [pause] and with verification methods to confirm that the user is genuine.

It works along with and compliments current PCI standards and other Payment Security Technologies.

Yet as the rest of the world has adapted to these smart card technologies and EMV standards, the US has been slow to comply.

There are already 1.62 billion chip enabled cards now in circulation.

All bankcards that are issued in Europe already contain the chip.

The EMV transaction will be based on a secure microchip bankcard connecting to an EMV-enabled POS terminal.

This can occur either by a contact or contactless method. We will discuss these two techniques later in this course.

The smart card technology also provides an additional form of card authentication. It validates that the card is legitimate and that it is not counterfeit.

Let’s take a closer look at the Authentication process.

Authentication can occur in two ways: Offline or Online.

Offline Authentication will happen using three different methods:

1. Static Data Authentication (SDA)
2. Dynamic Data Authentication (DDA)
3. Combined DDA with Application Cryptogram (AC)

These are simply secure methods of communication that can occur between the smart card and the EMV enabled terminal without connecting directly to the bank.

There are restrictions to the number and the dollar amount of offline authentications based on the issuing bank.

Online authentication happens when there is an online connection similar to the way current magnetic stripe transactions are sent.

An important difference to note is that EMV uses something called an Authorization Request Cryptogram or ARQC.

This means that the information transmitted is unique to the user, the device and the transaction. It is also encrypted and can only be decrypted by the bank.

Some banks may require online authentication only.

The verification process confirms that the card holder is the one actually initiating the transaction.

There are 4 methods of verification:

1. Online PIN
   a. With this method, the PIN is encrypted and verified online by the card issuer.
2. Offline PIN
   a. Here, the PIN is verified offline by the EMV card itself.
3. Signature Verification
   a. With this process the cardholder signature on the receipt is compared to the signature on the back of the card.
4. No Verification
   a. This is typically only used for low value transactions or for transactions at unattended POS locations.

The verification methods are determined by the payment brand and the bankcard issuer in addition to the terminal type.

Combined with the process of Authentication, this is called 'Two Factor Authentication'. It involves identifying an item the user possesses [pause] and confirming something that only the user knows. For example the way an ATM requires both your card and your pin number to dispense cash.

Epicor plans to support both 'chip and PIN' and 'chip and signature' verification. The type will depend on the card brand used such as Visa, Mastercard, AMEX or Discover and issuing bank.

There are two ways that a smart card can be read; through Contact or with a Contactless method.

The Contact method requires the customer to insert the bankcard into the terminal device. The card must remain in the device for the entire transaction or the operation will be cancelled.

If a bankcard is swiped using the magnetic stripe reader, the terminal will be able to determine if the bankcard is actually a smart card.

If determined that it is, the customer will be instructed to insert the card into the reader.

With the Contactless payment type device, the customer simply waves the card over the terminal and then follows the prompts.

Epicor plans to support both Contact and Contactless EMV payments but will begin with Contact EMV payment initially and Contactless payments in Fall 2016.

EMV readiness is not as easy as just turning on a flag in your Eagle system or ordering a specific PIN pad.

Because of the increased security involved, the steps are more complex.

The good news is that this intricate process can increase your security and fraud protection, limiting your liability.

As your technology partner, we're here to either guide you along the way or to manage it for you.

Learn more about EMV here.

This link can also be found in the EMV Frequently Asked Questions document located in the course materials section for this Training on Demand class.

EMV is an Eagle enhancement and there is no expectation of any additional charges related to software.

However, depending on the configuration of your PIN pads, there may be debit key encryption fees associated with the EMV conversion.

Consumers and businesses want more bankcard security and a reduction in fraud.

EMV is a standardized set of specifications designed to deliver both.

By upgrading your software and checking verifying your readiness, you will be well prepared for the transition toward a more protected data environment.