Merchant Guide to Modernizing Your Payment System

May 2017

A collaboration between:

BOOMTOWN! | DISCOVER GLOBAL NETWORK | ETA ELECTRONIC TRANSACTIONS ASSOCIATION

Disclaimer

This 'Merchant Guide to Modernizing Your Payment System' (this "Guide") assists U.S. merchants deploying EMV at their point-of-sale (POS) with information to help work with merchant services providers, integrated POS vendor, and dealers to accept chip cards in store. This guide provides high level information and only relates to card present transactions. It is subject to change at any time without notice. Neither this Guide nor any other document or communication creates any binding obligations upon any party.

This Guide is provided "AS IS", "WHERE IS" and "WITH ALL FAULTS". Neither, nor any of its members, directors, officers or employees (collectively, the "ETA Parties") assume or accept any liability for any errors or omissions contained in the Guide.

The ETA Parties specifically disclaim and make no representations or warranties of any kind, express or implied, with respect to this Guide including implied warranties of merchantability and fitness for a particular purpose. The ETA Parties further specifically disclaim all representations and warranties with respect to intellectual property subsisting in or relating to the Guide or any part thereof, including but not limited to any and all implied warranties of title, non-infringement or suitability for any.

Contents

Introduction – Modernizing the Point-of-Sale

This Manual is intended to help merchants modernize their point-of-sale payment system to support chip card acceptance. The objective is to be a hands-on guide for facilitating discussions between the merchant service provider (MSP), the processor, and the dealer to provide solutions for in-store card-present transactions. We start with a recap on EMV or chip card acceptance which is a "must" for any terminal system to be considered modernized. Best practices are then outlined which includes information related to data security applicable to chip card transactions consisting of tokenization, encryption, and PCI data security standards. Then, a guide covering six steps is offered to assist with the POS system transition – from reviewing the current payments system to training employees.

Chapter 1: EMV Recap

What is EMV and Why is it Important?

The U.S. payment card industry is in the midst of a major transition to supporting EMV while other countries across the world have previously implemented EMV. EMV is chip card technology overseen by EMVCo, a global payments industry body that manages, maintains and updates EMV Chip Specifications, for both contact and contactless payments, to facilitate interoperability and enable payments between chip-based payment applications and POS acceptance terminals. The organization is made up of six members: American Express, Discover, JCB, MasterCard, UnionPay and Visa.

Support for EMV is important because chip cards lessen the risk of fraud compared to magnetic stripe cards. An embedded microchip uses dynamic data during each transaction, which makes them difficult to counterfeit. On June 23, 2016, EMVCo reported that by the end of 2015, the number of EMV payment cards in global circulation increased, year on year, by 1.4 billion to 4.8 billion. The UK Cards Association said according to the EMV FAQ produced by *EMV Connection*, "Fraud on lost and stolen cards is now at its lowest level for two decades and counterfeit card fraud losses have also fallen and are at their lowest level since 1999."

Implementing chip card technology on POS Terminals helps protect against in-store card present counterfeit and lost/stolen fraud. Chip card technology is different than point-to-point encryption (P2PE) and tokenization. Point-to-point encryption and tokenization are technologies that help protect card transaction data stored on merchants' systems and card transaction data in transit transmitted to and from POS Terminals to help reduce the risk of data breaches respectively. Each merchant should evaluate its fraud concerns to determine a holistic fraud prevention strategy. Point-to-point encryption and tokenization solutions help protect merchants when breaches occur of static and in-transit card transaction data.

There are two main types of in-store card present fraud that chip technology helps reduce:

- Counterfeit Cards – Unlike magnetic stripe cards, chip cards are difficult to counterfeit because of an embedded microchip that exchanges unique, dynamic data with a terminal each time it's used.
- Lost & Stolen Cards – By supporting terminals accepting PIN preferring chip cards, merchants may be in a position to shift liability for lost and stolen fraud in accordance with payment network rules.

Even for small to medium-sized merchants, accepting chip card payments is important. As large, nationwide retailers have implemented this technology, fraud could shift to less-protected channels, so terminals that have not been upgraded to accept chip payments could become a target.

How Does Chip Technology Make Payments More Secure?

Chip technology makes in-store card present transactions more secure than transactions with magnetic stripe cards because:

- **The chip helps prevent card cloning** – it is harder to duplicate than a magnetic stripe card
- **Cryptography**:
    - In each card transaction, various cryptograms are generated based on public keys loaded in the terminal and in the card
    - Every time a card is inserted or a contactless device is tapped, it is validated.

Cardholder Verification Methods:

Before chip card technology was available, payment cards were produced with just a magnetic stripe containing minimal cardholder information. Cardholder verification at the point of sale was limited to using signatures. Since U.S. cardholders are familiar with magnetic stripe cards and providing their signature for verification with a card transaction, in an effort to reduce complications at the POS in the U.S., most U.S. credit card issuers are issuing chip cards that require a signature for cardholder verification rather than a PIN.

However, when selecting terminals for a modernized payment system, you should require support for cardholder verification options that are flexible enough to address current technology supporting current and future needs of your customers. PIN acceptance for online entry and also for when the terminal is offline to help reduce fraud are key features as is support for acceptance of contact and contactless chip card transactions. Deploying comprehensive terminal support for cardholder verification methods should ensure the system supports acceptance of current card technology and helps manage fraud.

Chapter 2: Best Practices for Modernizing your Payment System

As you begin to plan your transition to modernize your payment system, current best practices and a step-by-step guide are provided to assist with a smooth transition.

Start planning early

- As you transition to modernize your payment system, you have several factors to consider that can impact your business and your customers. For example, upgrading to an entirely new POS system instead of buying new terminal hardware may impact how you run your business so you should plan ahead.
- Discuss EMV readiness with your terminal provider to understand their ability to support the entire EMV transaction from card to processor when setting deadlines for your transition.

Plan for the future

- When selecting terminals, consider options that allow you to support the current and future needs of your customers, such as contactless payments, PIN, rewards and loyalty programs.
    - Confirm that your POS hardware is capable of supporting contactless payments so you can accept mobile wallet transactions, such as through Apple Pay and Android Pay.
    - As the industry moves to supporting EMV, many issuers will issue PIN preferring chip cards, such as debit chip cards. Confirm that your terminals have PIN pads that are PCI PIN Transaction Security (PTS) compliant. Contact your payment provider to ask about your ability to accept PIN payments and certification requirements.

Understand your needs when discussing options with your MSP or payment processor

With hundreds of hardware and software options in market, make sure you are getting the technology that is right for your business and your customers. **Select vendors carefully.**

- Before selecting your vendors, make sure that an acquirer/payment processor and integrated POS solutions can provide the POS hardware and software functionality that you want, as well as the support you need for a seamless transition and continued success.

Understand how PCI Data Security Standards (PCI DSS) and EMV work together

- EMV, Point-to-Point encryption, tokenization, and PCI function best when they are combined. When used together, EMV, Point-to-Point encryption, tokenization and PCI compliance may reduce fraud and enhance the security of your payments infrastructure.
    a. An EMV chip has security features that can reduce counterfeit card fraud at in-store card-present environments. Plus the support for PINs can help merchants shift liability for lost and stolen fraud for card present transactions under payment network rules.
    b. Point-to-Point encryption is used to protect card data by encrypting it at the POS from the time the card or contactless device is swiped/inserted/tapped in the POS Device until it is decrypted for authorization.
    c. Tokenization helps protect merchants when breaches occur of static data.
- PCI provides other complementary levels of security to protect sensitive cardholder data within the payment ecosystem, thus limiting the availability to fraudsters. Please visit the PCI Security Standards

website for various education materials on this topic:
https://www.pcisecuritystandards.org/pci_security/educational_resources

Do you need to get your system certified?

Every chip-enabled terminal must be certified by EMVCo and end-to-end (E2E) certified by the payment networks you want to accept. The size and complexity of your business will determine the level of certification required. Unless you have hundreds or thousands of locations and a highly customized POS software (fully-integrated), it's likely that you won't have to play a major role in the certification process.

If you are required to obtain certification for your POS system you will want to work with your acquirer to help guide you through that process. It can include needing:

- E2E terminal certification to be completed for each payment network supported by the terminal.
- Each terminal application you use, combined with any middleware software product, should be certified by each processor.

The purpose of E2E testing will be to:

- Demonstrate that the deployed POS terminals meet the requirements of both the acquirer and payment networks.
- Send authorization requests and receive authorization responses between POS terminals, acquirer host systems and payment networks.
- Demonstrate that POS terminals can process chip-based functions including PINs, fallback transactions and CVMs as supported by the POS terminal.

Chapter 3: Step-by-Step Guide for Your Business

We have provided a step-by-step guide for your business to assist with your transition to modernize your point of sale. Here are the steps that we will cover in the following pages to help ensure you address the key considerations:

1. Review your current payment infrastructure.
    a. Write down all the hardware and software enabling your business to process payments.
        i. Note all of the involved vendors.
    b. Record the details of the network that powers your internet connection for your business.
2. Determine your goal of the hardware/software upgrade.
    a. Are you happy with your current set-up or do you want more functionality? Be specific.
    b. Are you willing to pay a premium for better, more secure POS software and hardware?
    c. Do you want to future-proof your hardware or just get the required minimum?
3. Discuss your options with your MSP and/or payment processor and questions:
    a. See what's out there. Get recommendations from the experts.
    b. Does the new technology meet your payment security goals?
    c. Can it accept all the forms and channels of payment that you desire?
    d. Will you need additional certifications and testing? (Your gateway, processor, or POS software provider may be responsible for this if you are utilizing a semi-integrated solution.)
    e. What will the installation and configuration entail? Do they provide assistance?
    f. Will you need a new or upgraded secure wireless network to support the hardware?
    g. Is there training and ongoing support available for your new technology?
    h. How will the new hardware impact your daily workflow?
    i. What type of ongoing support will they provide? Have those terms been agreed upon contractually?
4. Install your new hardware.
    a. Get your new system properly installed and configured. Consider hiring Qualified Integrators and Resellers (QIR) to assist with the installation. QIRs receive training and qualification on the secure installation of Payment Application Data Security Standard (PA-DSS)-validated payment applications into merchant environments in a manner that facilitates PCI Data Security Standard compliance.
    b. Make sure your network is reliable and secure.
5. Get your system certified (if applicable)
    a. To learn more about certification, visit PCI Security Standards Council: https://www.pcisecuritystandards.org/
    b. Each POS terminal application, combined with any middleware software product, should be certified by each processor.
    c. Finalize your PCI compliance as soon as possible.
6. Train your employees and your customers
    a. Make sure your cashiers and/or wait staff know how to accept chip cards to assist your customers.
    b. Take advantage of marketing and educational materials for merchants such as those found at: http://www.discovernetwork.com/chip-card/vars/resource_center.html.

Review Your Current Payments Infrastructure

Shifting to chip technology provides an opportunity to take a comprehensive look at your payments capabilities so you can accept new forms of payment in the future. Since you will likely be purchasing new POS hardware to accept chip payments, it is a great time to get hardware that enables other forms of emerging payments that consumers have shown interest in, such as mobile payments. Beyond payments capabilities, could your business benefit from a more holistic POS solution that can track inventory, provide loyalty solutions, and much more? If so you may be interested in such functionality in addition to acceptance support.

When you're ready to get started, the first step is to walk through the list below and document the existing payments ecosystem at your business:

- What brand(s) of hardware do you currently use to accept payments at your business?
- How many devices do you have? Do you use a stand-alone payment terminal, or is it attached to (or integrated into) your point-of-sale system?
- What payment channels do you have in place (in store, online, mobile, mail order, etc.)?
- Who is your acquiring bank?
- Who is your payment processor?
- Who is your POS provider (if applicable)?
- Do you use a gateway, middleware provider?
- Who do you call for technical issues?
- What debit/credit card brands do you currently accept at your business?
- Do you use wired or wireless internet to power your payment terminal and POS system?
- Is the network you use to process payments secure?

Before you move on to the next step, answer these questions thoroughly. The answers will guide your future conversations with your merchant services group and payment processors.

Determine Your Goals and What You Want From Your New POS Hardware/Software

One of the hardest parts of the transition to chip technology is deciding on the right POS hardware and software for your business. Are you looking strictly for a way to accept chip cards with no additional frills, or do you want a full POS system to manage your entire business operation?

If your business already has EMV-capable terminal(s) in a stand-alone environment (see below) or a need to swap out non-EMV terminal(s) with ones that are EMV-certified, then the transition will likely be seamless with minimal costs. If you're thinking about upgrading your existing system to something more robust or integrating EMV into an existing POS system, will require a few additional decisions.

Let's take a look at the three main options you have for an upgrade.

- **Stand-alone solution** – This is the most basic set-up. If you only want to be able to accept chip cards and nothing else, this is the easiest, cheapest and fastest option. Just swap out your non-EMV terminal(s) for an EMV-enabled POS terminal. Keep in mind that this option offers the least amount of functionality. It's worth noting that even with a stand-alone solution, you can still accept contactless payments if you select the right hardware.

- **Semi-integrated solution** – This is the most common set-up for many businesses. A semi-integrated solution is one in which a payment terminal is used to capture card transaction data and process payments, but it is connected to a POS application (often residing on a PC or register) rather than being a stand-alone device. This approach is generally straightforward because the EMV processor certification and integration to the POS are often completed by the terminal provider and software application provider. In a semi-integrated environment, the POS software applications can be often be changed more easily and sometimes reduce recertification needs of the application. However, every initial EMV application requires E2E certification with each card brand. Since payment data transmission is limited to the payment application and the processor (i.e. sensitive data never enters the POS application), semi-integrated approaches can potentially take POS applications out-of-scope for PCI certification regulations as well.
- **Fully-integrated solution** – The fully-integrated approach is the most complex integration and not as common for small businesses. There are two main uses cases where you may want to consider a fully-integrated solution:

  1) You process millions of transactions per day and are looking to reduce payment gateway fees associated with a semi-integrated solution.

  2) Your business model (i.e. large fine-dining restaurant) requires to support specific needs to minimize the impact on workflow

In a fully-integrated solution, the payment application is an integral part of the core POS solution. One piece of software handles every aspect of the transaction, which means each terminal is not separated from the rest and a card can be authorized and closed out on separate terminals. In this scenario, the entire payment system (POS, terminals, servers, firewalls, etc.) is within the business's own infrastructure. This also means that the entire system is within PCI scope and a change made to any part of the system affects the other parts. Encrypted card holder data and transactional data is being stored on the system, and being sent for processing through your internet connection. EMV adoption will influence the approach to payment application integration, because every EMV acceptance application requires end-to-end certification with each card brand. Therefore, in a fully-integrated environment, any modification to the core POS brings the potential that recertification might be necessary, even if the payment-specific part of their application goes untouched.

If you are interested in a **stand-alone** or a **semi-integrated** approach, here are a few questions that you should ask yourself as you determine what hardware is right for you.

Are you willing to pay a monthly fee for added benefits and functionality (cloud-based POS solutions typically average around $50/month per terminal, but can be more)?

Yes, I am.	**No, I am not.**
No one likes to spend unnecessarily, but the operational efficiencies that come from a full point-of-sale system can be dramatic and may ultimately save you time and money. Now that you have decided that a new point of sale system is right for you, write down a list of all	If you're not willing to spend extra, but you are still interested in added functionality, there are a few options that offer robust solutions without a monthly fee. Keep in mind that with these bundled solutions, you will likely pay higher processing fees than you would through your current payment processor. You can run an analysis based on your

the functionality that would help your business. Here are a few ideas: • Inventory tracking • Item discounts • Automated marketing solutions • Integrated accounting software • Barcode scanning • Dynamic table service and bill splitting • Loyalty programs • Sales analytics • Mobile table-side ordering	processing volume to see if it makes monetary sense for you to go this route.

It's also a good idea to prioritize your desired functionality from most important to least important. This will allow you to conduct the best cost/benefit analysis when you are deciding on a system.

Once you outline needs, you are ready to discuss the list with your MSP or payment processor. They will be able to recommend solutions that would work for your specific business type. You can also do your own research online to compare software products and get a sense of what is available.

Do you want to anticipate future card acceptance needs of your business by being able to accept contactless payments like Apple Pay, Android Pay, and Samsung Pay? Do you want to be able to accept chip and PIN in addition to chip and signature?

Yes, I want to address the future card acceptance needs of my business technology.	**No, I'm not interested in new payment technologies.**
You will want hardware that can accept contactless payments, which is what many mobile wallets use to trigger payments from mobile phones You will also want to make sure that your terminal supports all CVMs including PIN to avoid responsibility over lost & stolen fraud.	You will only need a terminal that supports chip card acceptance and is capable of supporting current Cardholder Verification Methods. Note that you may need to purchase new hardware again in a few years.

At this point you should have a good understanding of what payment hardware is right for your business. Once you feel comfortable that you know what you're looking for, continue on to the next step.

Discuss Options with Your Merchant Services and/or Payment Processor

Now that you have taken inventory of your existing hardware and determined what you want from the upgrade, it's time to talk to your MSP, payment processor, and POS provider (if applicable). Your merchant services team knows your business volume and they have the most insight into what is and isn't working in the market today. They are also incentivized to make sure that you are successful, because the more successful you are, the better they do. You should clearly outline everything that you want your new payment infrastructure to accomplish and ask them for advice. Most acquirers and processors today have hardware options that range from the most basic terminals through highly customizable cloud-based POS systems.

The first step is to get advice on the right hardware for your business based on the information you outlined in the previous step. Once you outline your needs to the vendors, here are a few questions to ask to get you started:

- Based on the functionality I outlined, what is your opinion of the best solution for my business?
- What payment forms will my new hardware be able to accept? Chip and signature, chip and PIN, magnetic stripe, contactless payments?
- What is the cost of hardware to become certified?
- How long will the hardware take to arrive?
- Will it come pre-configured? If not, what do I need to do when it arrives?
- Will the new hardware be wired or wireless?
- What does the installation entail?
- Do you provide any installation services? If so, are you a Qualified Integrator or Reseller (QIR)?
- Will you train me on how to use the new system once it is set up?
- Do you provide ongoing support in case I have questions about the new technology and are there fees?
- How will the new hardware impact my existing work flows (e.g. will my staff need to return to the same terminal to authorize and close out a bill)?

While you're focusing on getting the right hardware for your business, it's also important to address your security concerns in addition to the necessary functionality.

EMV is an essential component of an in-store payments environment that mitigates security risks, but it's only one piece of the puzzle. You also want encryption and tokenization to bring additional layers of security to your payment environment. But, what does that mean?

Encryption –PCI Data Security Standards requires encrypting card transaction data stored on your systems and transmitted over a public network. Card transaction data can also be encrypted within the terminal to help protect data from unauthorized access inside of a merchant environment. Card transaction data is transmitted with encryption all the way to the processor or service provider, where it can be decrypted. If encryption is properly implemented, the merchant's systems (outside of the terminal) will not handle any clear-text card data reducing the risk of security breaches.

PCI Security Standards Council (PCI SSC) has introduced a voluntary program called the PCI Point-to-Point Encryption Program (P2PE). Encryption solutions that are PCIP2PE-validated are required to follow rigorous standards. POS software systems which are integrated with such PCIP2PE payment systems are kept out of scope for PCI DSS compliance because the sensitive card data never enters the Merchant system, but rather the data is encrypted at the point of interaction. Please visit PCI SSC website to get the current list of solutions that comply with PCI P2PE standards. https://www.pcisecuritystandards.org/.

Tokenization – Tokenization products devalue card transaction data by replacing the Primary Account Number (PAN) with a token. When developed and used as specified, these solutions may reduce for merchants by removing the need to store valuable card numbers in their networks and systems. Tokenization products include hardware devices, software applications and service offerings.

The security objective of a tokenization process is to ensure the resulting token has no value to an attacker. When evaluating a tokenization system, it is important to consider all elements of the overall tokenization implementation. These elements include the technologies and mechanisms used to capture cardholder data, how

a transaction moves through your environment, the transmission from the point-of-capture (e.g., point-of-sale system) to the authorization endpoint, how tokens are retained for use (e.g. in back office systems) and so on.

Breach Insurance - It's important to ask questions to confirm that your new payment infrastructure is designed for long-term success. While breach insurance may be of some value to the merchant community, it is crucial to understand that it is not sufficient protection from the reputational and financial impact of a data breach. Breach insurance should not be considered an alternative to adoption of chip, encryption, tokenization or other layers of security set up for long-term success.

Questions to ask regarding the security of your new system:

- Is the system you're recommending EMV-certified?
- Does the solution provide point-point encryption, support tokenization and is listed with the PCI Security Standards Council listing?
- Do I need to play a role in EMV certification based on my proposed payment solution? If so, how long will it take and how much will it cost? Note that E2E certification is required for every hardware/software/platform combination (See the "Get Your System Certified" section earlier in this document.)
- Will I need additional hardware beyond the terminal to secure the transaction data?
- Has the terminal been certified under the Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) process for version 3.1 or most current version?
- Is the POS software approved and listed as a being compliant with the PCI Payment Application Data Security Standard (PA-DSS)?

Once you're satisfied that your proposed hardware will meet all your desired functionality and security needs, it's time to place the order and get ready to make the transition. If you are selecting someone to install your new system it is important to familiarize yourself with the PCI QIR Program.

QIR Program:

Organizations qualified by PCI SSC as Qualified Integrator and Reseller Companies (QIR Companies), such as Boomtown, are authorized to implement, configure, and/or support validated PA-DSS Payment Applications on behalf of merchants or service providers for purposes of performing Qualified Installations as part of the QIR Program. The quality, reliability, and consistency of a QIR Company's work provide confidence that the Payment Application has been implemented in a manner that supports the Customer's PCI DSS compliance.

It is important to note that the incorrect installation and/or maintenance of payment applications can create opportunities for merchant's systems to be compromised. Integrators and resellers play a key role in the payments ecosystem, as merchants depend on these service providers to install, configure, and/or maintain their validated applications.

Resellers are highly encouraged to pursue QIR training and certification, and merchants should use a QIR to install their devices - as it improves security by validating that payment applications and terminals are installed and integrated in a manner that mitigates payment data breaches and facilitates a merchant's PCI Data Security Standard (DSS) compliance. Using QIR companies provides small merchants some protection against common compliance matters. Information can be found at the PCI Security Standards Council website. https://www.pcisecuritystandards.org/.

Install Your New POS Acceptance Hardware

The complexity of the installation will depend on the type of POS acceptance system that you have chosen. If you're adding a new terminal, it should be plug-and-play installation with a potential software update (as long as the hardware comes pre-configured for your business). Your merchant services team or the POS provider should be able to guide you through that process.

If you're setting up a new POS system, is the system wireless or hard-wired (connected with an Ethernet cord)?

If it's a wired system, the installation may entail running some new Ethernet cables. With a hard-wired system, you will have fewer concerns related to the security of your network, but the general flexibility of the system is reduced.

If you are moving from a wired to a wireless system, the first thing you need to do is to make sure your network is reliable and secure in order to seamlessly power your payments. Below you'll find some questions you can ask to make sure that your wireless network is properly configured for your business needs.

- Is my internet fast enough to power my new system?
    - You can conduct a free network speed test by going to: http://www.speedtest.net/
    - While pure payment processing doesn't require significant download and upload speeds, if you want your new wireless point of sale system to run smoothly, we recommend, as a rough guide, having at least 3Mbit/s downstream speed and 1.5Mbit/s upstream speed per point of sale device. This should ensure a smooth connection for your point of sale system.

- Is my signal strong enough at the location of each terminal?
    - Your system should provide wireless signal strength no less than -70 dbm to each wireless terminal in any location where the terminal will be in use. If you are planning to have mobile terminals (e.g. tableside ordering), you will need a strong and consistent signal strength throughout your business. If you need a stronger signal in certain areas of your business, you can add additional access points to your network that will expand your Wi-Fi coverage.

- How do I install the Ethernet cable to connect the routers and access points to the modem?
    - You can purchase pre-cut Ethernet cords to connect your network hardware if the distance isn't too far. If you want a custom wiring job, you will need a spool of CAT5 cable, a cable stripper and crimper, a punch down impact tool, RJ45 tips, and a cable test kit. These tools will allow you to cut your desired length of CAT5 cable, add the tips and run it between your network hardware in your business. You may want to mount the cables with surface mounts and use a U-shape stable gun to hold the cables in place for a cleaner and more dynamic installation. Professional cabling is always available from Boomtown's local technicians if you need assistance.

- What are some things I should keep in mind when setting up my wireless network?
    - Generally it's not advised to use ISP-provided modems/routers because they tend to be low quality and are often years out of date. They also may not have the functionality and security features that you want for your business. Finally, you will likely pay more over the life of the router to rent it from the ISP than to buy it yourself.

- Do not use multiple network routers in a chained configuration, even if one is being used as an access point. These should be replaced with proper access points connected to your modem or switch.
- If you are going to provide Wi-Fi access to your customers, you must separate that network access from the network that your point of sale and payments devices are on. You can use a separate router for each network or you can use a dual-band router that has built-in security features.
- If you need network hardware recommendations, Boomtown is happy to provide guidance based on your specific business type and needs.

- How do I minimize the risk of unauthorized access to my wireless network?
  - **Encrypt your system**. Use at minimum WPA2/PSK encryption to secure your system. This is the most trusted encryption today for small business networks and it will add a password to your network.
  - **Get a firewall**. A properly configured firewall acts as the first line of defense in any network. It allows you to close off ports that aren't being used by your business. The good news is that most business routers have built in firewalls so you can log into your router and configure your settings directly.
  - **Set a password for your firewall**. The firewall doesn't do any good if it easily bypassed. This can happen if you keep the default username and password, which can be changed from the admin section of the router.
  - **Update Router Firmware**. Router/firewall firmware can become dated within a year. It's important to update to the latest firmware to maintain security. This can easily be done on the administration view of most modern routers.
  - **Disable SSID**. This option decides whether or not people can see your wireless signal. Since you aren't using this network for a guest network, you should hide it to the outside world.
  - PCI DSS includes several requirements in regards to wireless connectivity. Review these carefully to validate you have properly configured your wireless networks and firewalls to protect cardholder data.

Once your network is properly setup to limit unauthorized access, you can install the point of sale hardware, if that's what you ordered. There are some basic components that will be required and the installation process will vary depending the complexity of your system. Here's a general guideline of what a point of sale installation entails:

- Set up the payment stations or tablets
  - If the stations are wireless, these can be placed anywhere in your store that you have significant wireless network coverage.
  - If the stations need an Ethernet connection, you will need to run a cable from the network hardware to each location to connect the system to the network.
- Set up the peripheral devices (payment terminals, cash drawers, barcode scanners, receipt printers).
  - Once the stations are in place, you will need to connect all the peripheral devices to the core network. The peripheral devices can often be connected with cords that are provided with the hardware.
- Install the printers (if applicable).

- It is generally a best practice to run a cable to connect your printers to your point of sale system because the wireless signal can be weak or inconsistent. The last thing you want is to slow down business because your wireless connection on your printer dropped.
- This entails installing a separate cable for these printers, which takes more time but will provide a better experience over the long-term.

- Configure the software
  - Now that your hardware is properly setup, you will need to configure all the peripheral devices that you purchased to function as you want them to. This will include making sure your terminal processes payments, your receipts print to the correct printers, your barcode scanners enter information correctly to your software, and your cash drawer opens when you need it to.

Once your hardware and network are setup correctly, you're ready to validate your new system and ensure your compliance with the necessary standards. You can take advantage of free Discover Production Validation test cards to confirm your terminal/peripheral is working properly for EMV. Follow this link to request your test cards: http://www.discovernetwork.com/chip-card/images/EMV%20Test%20Card%20Request%20Form.pdf.

EMV & PCI Compliance – Will EMV Make you PCI Compliant?

It is not only POS software that matters for PCI compliance, the entire business operation contributes to PCI compliance. This includes, but is not limited to, hardware, software, and internet connectivity as well as people and processes. Based on brand compliance requirements, in a stand-alone or semi-integrated scenario, you may be able to complete a self-assessment questionnaire (SAQ) for your attestation of PCI compliance. Note that this would only be in cases where a PCI listed P2PE solution has been properly implemented and no card data is stored elsewhere through other channels. Be sure to check with your acquirer regarding the details of your specific requirements.

PCI has launched a small business taskforce to provide additional guidance for merchant to improve their security. Please refer to this link for information: https://www.pcisecuritystandards.org/pci_security/small_merchant.
PCI has published several guidance papers on securing wireless, accepting card transactions on telephone etc. Please refer to https://www.pcisecuritystandards.org/document_library.

Train Your Employees and Customers

Finally, once your new system is installed and your network is secure, you need to train your employees how to use the modernized POS system. For example, when you introduce EMV you should expect:

- For most terminals, chip cards are inserted chip-first and chip-side up.
- Chip credit cards must typically remain in the terminal for the entire length of the transaction. Employees should advise customers to follow terminal prompts that indicate when the card should be removed.

For this new technology, it is important that, in addition to training your employees, you capitalize on opportunities to train customers. Running a pilot program will be important as new processes will take time to get used to, and there may be a number of questions from customers.

Designate experts among your team to understand payment options

Identify and train staff to be the experts in the different payment methods, including EMV and contactless payments, so they can help store employees and customers. An expert with the new POS system must be able to understand how all components work together, how to troubleshoot and correct issues, and be able to escalate to ensure questions and problems are resolved.

Discuss the checkout processes for chip cards with store managers and employees

Chip cards may process differently from each other when used at the terminal. That's because some card issuers will have a PIN behind their card, and others might have a signature. Be sure to educate all employees on how the transactions might work once customers start using their chip cards. And always remember to indicate for customers to follow the prompts of the terminal.

Also, luckily, if a customer swipes a card that has a chip, EMV-enabled terminals will recognize the card has a chip and prompt consumers to insert the card.

Walk through the transition to chip cards and any other recent terminal updates

Recently, new payment methods have been introduced in addition to chip cards, such as mobile wallets, so it's important to keep employees well-trained on the latest POS terminals and devices.

When educating your staff on the transition, walk through the go-live date for chip card acceptance in your store, but also remind employees about each type of payment your store accepts, from chip cards to contactless payments to mobile wallets, so no one accidentally turns away a certain payment type at checkout. Periodically gather employee feedback to identify potential issues with a certain card brand/payment method, etc.

Leverage videos, store signage, and other useful industry resources

Educate employees further by using trusted industry resources. To help navigate through this new environment, Discover Network can help you to better understand chip cards and EMV-enabled terminals and other changes to the industry.

You can visit the Discover Network EMV Resource Center, which provides many free resources to prepare for your migration to EMV, including a training video. Discover Network also offers in-store signage to place on EMV-enabled terminals, windows, and counters. To view this signage, visit the Merchant Resources Center at http://www.discovernetwork.com/chip-card/merchants/.

Remind employees about the power of friendly customer service

A trained staff, some patience, and friendly customer interaction can go a long way as the industry collectively migrates to new and safer payments technology.

Encourage employees to be attentive to each customer and each transaction, especially as consumers have varying degrees of knowledge about chip cards. By providing an exceptional level of customer service, you can truly make your business stand out from the rest, gain competitive advantage, and keep customers coming back.

Despite best efforts, fraud can happen so merchants should continue to be vigilant. Below are some suspicious behaviors by in-store customers that may indicate a fraud attempt.

- Makes random purchases without paying attention to size, value or price
- Presents you with a card taken from a pocket instead of a wallet
- When asked, claims to have left photo identification at home or in the car
- Arrives at or about closing time and tries to hurry you through the sale
- Purchases a large item and refuses delivery
- Displays no interest in the warranty on expensive items
- Is overly slow and deliberate when signing the sales draft, perhaps because the signature is being forged
- Attempts multiple cards in a short time period

CONCLUSION

This guide to modernize payment systems focused on support for chip cards acceptance and card transaction data security risks. Many important steps and useful links were included to help you build a solid payment system foundation and prepare for the future. Select your needed partners carefully using this information to facilitate discussions which will help ensure an effective transition to a modernized payment system.

Appendix A

Glossary of Terms

Term	Definition
Acquirer	An entity that is permitted by the payment network to offer acceptance of credit, debit and prepaid cards to Merchant.
Acquirer Processor	A third-party entity operating as agent of an Acquirer for the purpose of performing certain Acquirer obligations in connection with card transaction.
Cardholder	A person to whom a credit, debit or prepaid payment card product is issued or an authorized user of such card.
Chip Card	A card with an embedded integrated chip that is a contact chip payment device, a contactless chip payment device or a dual interface payment device.
Chip Card Transaction	A card transaction that takes place with a chip card at a chip card terminal that complies with relevant operating regulations and technical specifications.
CVM	Cardholder Validation Method used to ensure that the person presenting the card is the person to whom the application in the card was issued.
EMV	The global standard for credit and debit payment cards based on chip card technology. EMV is a trademark owned by EMVCo, LLC.
EMVCo	The corporation that manages, maintains and enhances the EMV ICC specifications for chip-based payment cards and acceptance devices, including POS terminals and ATMs.
Merchant	An entity engaged in commercial operations that comply with the requirements set out in the Discover Operating Regulations and other program documents.
MSP	Merchant Services Provider.
Payment Network	An organization that manages a network to facilitate payments between Cardholders and Merchants.
PTPE	Point-to-Point Encryption. A solution provided by a third party solution provider, and is a combination of secure devices, applications and processes that encrypt data from the point of interaction until the data reaches the solution provider's secure decryption environment.
Payment Device	Contactless D-PAS products can be issued in many different forms such as key fobs, stickers or mobile phones. These devices are collectively known as "contactless payment devices."

PCI	Payment Card Industry Security Standards Council. A global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.
PIN	The personal identification number or code assigned by an Issuer that may be used by the Cardholder to facilitate a card sale or cash advance on a POS device.
POS Device	An electronic card reader, chip card terminal, cash register or terminal and any necessary software, located at the physical premises of a Merchant that is capable of electronically capturing data from cards and receiving electronic evidence of authorization responses and which may also be capable of transmitting electronic evidence of sales data.
Terminal	An electronic device that accepts and processes payment transactions.
Tokenized	Substituting a sensitive data element with a non-sensitive equivalent, referred to as a token.
VAR	An entity that adds features or services to an existing product, then resells it (usually to end-users) as an integrated product or complete turnkey solution.