Visa U.S. Merchant EMV Chip Acceptance Readiness Guide

10 Steps to Planning Chip Implementation for Contact and Contactless Transactions

Visa U.S. Merchant EMV Chip Acceptance Readiness Guide

10 Steps to Planning Chip Implementation for Contact and Contactless Transactions

Contents

About this Guide

What It Is

As the U.S. migrates to a contact and contactless EMV®-based infrastructure, merchants are encouraged to start thinking about the terminal upgrades they may need to support emerging chip technologies.

If you're planning to accept chip cards at your merchant location, there are a number of key factors to consider. How you proceed and when has a lot to do with your existing point-of-sale (POS) system capabilities and whether you own or lease your equipment. The *Visa U.S. Merchant EMV Chip Acceptance Readiness Guide* is designed for merchants who intend to implement EMV chip. Its primary purpose is to help you better understand the scope of an EMV chip implementation project—from start-to-finish.

The Guide follows a 10-step chip implementation planning process for merchants. This process is not meant to replace other chip-related Visa publications for merchants, but instead provides high-level guidance on how to better understand and prepare for the integration of EMV chip acceptance into your organization's daily payment processing operations and current project management processes. Merchants should continue to work with their acquirer and/or acquirer processor on their merchant migration requirements.

Who Should Use It

The Visa U.S. Merchant EMV Chip Acceptance Readiness Guide is intended for all merchants. However, it is particularly aimed at medium-to-large sized merchants who have integrated payment systems.

How It Is Organized

- Section 1: Introduction provides a high-level overview of the U.S. chip migration, as well as merchant payment system upgrade options and incentives. It also describes basic EMV chip technology integration solutions.
- Section 2: Chip Payment Processing Considerations – From a Merchant Perspective explains some of the key impacts that merchants need to take into account as they build a payment processing structure for chip acceptance. Description of key EMV chip implementation stakeholder partners is also included.
- Section 3: Building Your EMV Chip Acceptance Game Plan highlights 10 major steps you can take to assess the readiness of your payment system infrastructure for the chip platform, and understand what's required when making a fundamental shift to chip technology. These steps are based on merchant chip implementation efforts and lessons learned in other markets where EMV chip has been successfully deployed.

- The Appendix at the end of this guide contains a list of additional chip implementation resources for merchants, a high level *Visa U.S. Merchant EMV Chip Acceptance Readiness Guide* checklist, and Glossary of Terms.

NOTE: The information in this guide is offered to assist you on an "as is" basis. This guide is not intended to offer legal advice, or to change or affect any of the terms of your agreement with your Visa acquirer or any of your other legal rights or obligations. Issues that involve applicable laws or contractual issues should be reviewed with your legal counsel. Nothing in this guide should replace your own legal and contract compliance efforts.

1. Introduction

As the Payment Industry Evolves, So Should You

The U.S. migration to chip technology is creating a strategic framework that supports future growth and value for all key stakeholders in the payment industry. For merchants who update their acceptance environment, it is an investment in more secure transactions and new business-building opportunities.

To accelerate the adoption of EMV chip technology in the U.S., Visa recommends card and terminal implementation solutions that support online (real-time) authorization, and the Cardholder Verification Methods (CVMs) of signature, online PIN, and No CVM (No Signature Required) for low-value, low-risk transactions as they are employed today in a magnetic stripe environment. By leveraging the ubiquitous telecommunications and strong existing payment infrastructure that already exists in the U.S., merchants will be able to deploy chip terminals in a reasonable time frame while enhancing security with EMV.

Additionally, contactless technology is presenting Visa with opportunities to provide enhanced payment services and new innovations in the payments arena. With a contactless interface, customers can make purchases by simply holding their Visa payWave contactless card or a consumer device, such as a mobile phone in front of a reader, rather than swiping or inserting it, thus making transactions faster and more convenient for both the customer and the merchant. Visa's contactless solution is both flexible and globally interoperable.

It Is a Small Chip with Big Benefits

A chip card is a plastic payment card with a microchip that is virtually impossible to duplicate. International market migrations to EMV chip have proven that chip cards help reduce counterfeit fraud. Chip technology heightens security through the use of stronger authentication that reduces the value of stolen data. The use of stronger authentication methods and unique transaction elements make chip card account data less attractive to steal and counterfeit fraud a near impossibility.

Merchant point-of-sale (POS) terminals can have contact and/or contactless chip reading device(s). Standards and data are consistent across contact and contactless terminals and cards.

- **Contact cards** communicate with the reader over a contact plate. The plate must come into contact with the terminal usually by inserting the card into a slot in the terminal. The card must remain inserted for the duration of the transaction.

- **Contactless cards** communicate via radio frequency (RF) and must contain an antenna.
- **Dual interface chip cards** combine both technologies and can communicate either way.

Visa chip cards also have a magnetic-stripe on the back to ensure acceptance at point-of-sale (POS) terminals that do not have a chip-reading device.

How It Works

Smarter Technology

Computer Microchip. A computer chip securely stores the card data that currently resides on the magnetic stripe. This makes it nearly impossible for a criminal to create a counterfeit EMV chip card.

Unique Cryptogram. The computer chip enables more secure processing by producing a one-time use code for each transaction.

Mobile Shopping. EMV technology will also enable a one-time use code for mobile transactions and support other security innovations like tokenization.

Added Security

Difficult to Counterfeit. Because EMV chip cards use cryptograms that are unique to each transaction, stolen chip card data cannot be used to create counterfeit cards.

Less Risk of Fraud. The added layer of security provided by EMV chips makes debit and credit card data much less valuable, decreasing incentive for fraudsters to steal data.

Zero Liability. With EMV chip cards, cardholders are still protected from fraudulent purchases with Visa's Zero Liability policy*.

Used Worldwide

130+ Countries. There are approximately 2.4 billion EMV chip cards in circulation and 36.9 million terminals active worldwide, ensuring you can use your account conveniently wherever you travel.

How To Use

Insert Card →
Instead of swiping, you'll insert the card into the terminal, chip first, face up.

Leave the Card in the Terminal →
The card must remain in the terminal during the entire transaction.

Sign the Receipt or Enter a PIN →
Either sign the receipt or enter your PIN to complete the transaction.

Remove Your Card
When the purchase is complete, remember to take your card with you.

Remember: The chip card still has a magnetic stripe, just in case you need to use it with a traditional terminal.

*The Visa Zero Liability policy covers U.S.–issued cards only and does not apply to ATM transactions, PIN transactions not processed by Visa, or certain commercial card transactions. Cardholder must notify issuer promptly of any unauthorized use. Consult issuer for additional details.

Visa's Roadmap to Chip Migration Success

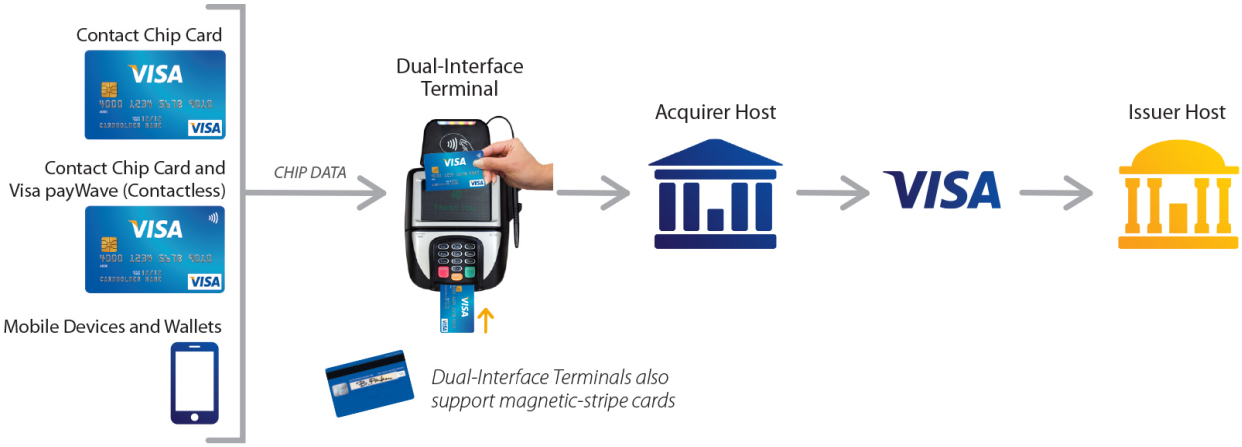
To help U.S. acquirers, acquirer processors, and merchants support chip and mobile payment acceptance, Visa has established the following incentives and mandates.

2012	2013	2015	2015	2017
Technology Innovation Program (TIP) Launch in U.S.	**U.S. Acquirer and Processor Mandates for Supporting Merchant Chip Acceptance**	**Debit/Credit U.S. Domestic and Cross-Border Counterfeit EMV Liability Shift for POS Transactions**	**Visa payWave Acceptance Contactless Reader Requirements**	**Liability Shift Expansion to Automatic Fuel Dispensers (AFDs) and ATMs**
Effective 1 October 2012, TIP allows merchants who update their POS infrastructure to waive their obligation to complete an annual Payment Card Industry (PCI) Data Security Standard (DSS) validation assessment. The elimination of this requirement could represent a significant cost reduction for participating merchants. While they still need to be compliant with the PCI DSS, merchants will not have to go through the process of validating compliance. TIP benefits qualifying U.S. merchants who process 75 percent of their transactions using fully enabled dual-interface terminals.	**Effective 1 April 2013**, acquirer processors and sub-processors must ensure their systems support merchant EMV chip acceptance by certifying their ability to carry and process the additional data in EMV chip transactions, including the cryptographic message that makes each transaction unique. Specifically, these entities must support Field 55 for V.I.P. authorization messages both at the host and POS level.	**Effective 1 October 2015**, Visa's global counterfeit liability shift will be instituted in the U.S for POS transactions. With this liability shift, the party that is the cause of a chip transaction not occurring (i.e., either the issuer or the merchant's acquirer processor) will be held financially liable for any resulting card present counterfeit fraud losses. The shift helps to better protect all parties by encouraging chip transactions that use unique, dynamic authentication data.	**Effective 1 January 2015**, Visa contactless readers connected to acquirer platforms that are certified for chip data no longer need to support the MSD transaction path. **Note:** New Visa payWave accepting contactless readers deployed between 1 December 2011 and 1 April 2013 must be configured to either: • Support only transactions as specified in VCPS 1.4.2, or • Actively support both the MSD and the qVSDC transaction path of VCPS 2.1, including all published updates, and transmit the resulting chip data to VisaNet.	**Effective 1 October 2017**, transactions made at AFD terminals and ATMs will be included in the Global EMV Liability Shift Policy.

Note: See Section 2 for April 2014 changes in liability for Unattended Cardholder Activated Terminal (UCAT) chip transactions.

What is a Dual-Interface Terminal?

Dual-interface terminals are able to process chip transactions from various payment products including contact chip cards, Visa payWave (contactless), mobile devices and wallets, and magnetic-stripe cards.



A Closer Look at Merchant Incentives for Point-of-Sale System Upgrades

Even though U.S. merchants are not required to support chip processing, there are powerful advantages for those who do. By updating their POS systems to accept contact payments, merchants are taking the necessary steps to be ready for the EMV liability shift. Effective 1 October 2015, Visa's global POS counterfeit liability shift will be instituted in the U.S. With this liability shift, the party that is the cause of a chip transaction not being conducted (i.e., either the issuer or the merchant's acquirer or acquirer processor) will be held financially liable for any resulting card-present counterfeit card losses.

Merchants may also want to build a future-proof infrastructure that will support emerging payment innovations, enhance global acceptance, and reduce risk. By encouraging merchant investments in dual-interface terminals through the *U.S. Technology Innovation Program (TIP)*, Visa is helping merchants advance to the next generation of electronic payment processing.

To qualify for TIP and receive its benefits, U.S. merchants must meet all of the following criteria:

- The merchant must have validated PCI DSS compliance within the previous twelve months or have submitted to Visa (via their acquirer processor) a defined remediation plan for achieving compliance based on a gap analysis.
- The merchant must have confirmed that sensitive authentication data is not stored. As defined in the PCI DSS, this includes the full contents of magnetic-stripe, Card Verification Value 2 (CVV2), and/or PIN data.
- At least 75 percent of the merchant's total transaction (chip and magnetic-stripe) count must originate from fully enabled dual-interface (contact/contactless) terminals that are capable of processing complete chip transactions.
- The merchant must not be involved in a breach of cardholder data. A breached merchant may qualify for TIP if it has subsequently validated PCI DSS compliance.

Enrollment in the TIP program is not automatic. Participation in the program is contingent upon an acquirer or acquirer processor's submission of a program application for a qualifying merchant and Visa's approval of that application. Visa will be working directly with acquirer and processors to confirm eligible merchants and verify acquirer and processor reporting responsibilities.

Merchant Payment System Integration and EMV Chip Solutions

The EMV chip implementation process for contact and contactless POS transactions varies by merchant type, size, and payment system infrastructure. POS integration can be as complicated as a state-of-the-art retail workstation or as simple as a basic till with an integrated card reader. Some merchants just need a "standalone" terminal with EMV functionality, while other large to mid-size merchants that have a more complex payment processing environment require customized payment network logic integration into their POS and point-of-interaction (POI) systems. Listed below are some of the merchant payment system integration considerations involved such as timelines, costs, flexibility and complexity.

There are three basic merchant payment system environments: Standalone, Semi-integrated, and Fully Integrated.

1. Standalone

Compared to integrated POS systems, a standalone POS device serves the single purpose of authorizing and clearing payment card transactions. Other names for standalone devices include electronic POS devices (although this also refers to integrated systems), or electronic data capture devices. A standalone POS device is usually not connected to a merchant's electronic cash register; rather, it connects directly to a host processor. For slightly larger merchants, the standalone device may be added to a cash register as a plug-in or stand beside device. Typically implemented by smaller (mom and pop) merchants, a standalone infrastructure is totally managed by the acquirer or processor, and as a result, only provides the options offered by that acquirer or process. It is easier to implement with minimal effort on the part of the merchant.

NOTE: While it is required to support the processing of transactions without a CVM, regular CVM processing protocol, in accordance with EMV, should be followed (i.e., if both the card and the terminal support PIN for point of sale, a PIN may be requested).

2. Semi-integrated

In this environment, the transaction acceptance device connects directly to the integrated POS device and runs on a local area network linked to the payment controller. A semi-integrated infrastructure is typically implemented by medium-sized merchants because it allows some flexibility regarding a choice of PIN pad manufacturers, acquirers, acquirer processors, and third-party vendors. It also offers other options such as a fully integrated environment, while reducing some of the complexity. It is, however, more challenging compared to the standalone environment. A merchant needs to weigh the options between the type of flexibility offered and the cost and time involved to implement.

3. Fully-integrated

In the fully-integrated configuration, the merchant's store's system controls all the components, and the integrated POS platform physically incorporates the transaction acceptance device. This environment maximizes a merchant's flexibility between the store systems' application and the payments software module (or middleware). This environment is typically implemented by major merchants, primarily because of the flexibility it offers when it comes to choice of PIN pad manufacturers, acquirers, acquirer processors, and third-party vendors. It is, however, more complex. A merchant needs to weigh the options between this kind of flexibility and the cost and time involved to implement.

How Contact Chip Card Acceptance Works Over VisaNet – Start-to-Finish

The diagram below illustrates the chip card payment processing infrastructure.

2. Chip Payment Processing Considerations – From a Merchant Perspective

Merchant Impacts

In the chip environment, the chip-enabled terminal and the chip card must agree on such processing issues as the card applications that are being supported (for example, Visa debit and credit, or Visa prepaid), any processing restrictions, the Cardholder Verification Method (CVM), and the card authentication that is being used. As far as EMV chip transactions are concerned, just think of all communication as a set of checks and balances between the card and terminal.

Listed below are some of the key impacts that merchants need to take into account as they build their payment processing structure for chip acceptance.

- **Card and Terminal Decisions.** The terminal and card interactive design process and final selection is based on a mixture of elements that are specific to that particular transaction, such as amount, domestic or international transaction, and other transaction parameters.
- **Cardholder Verification.** In the chip environment, merchants and cardholders rely on the chip-reading device and the chip card to agree on which Cardholder Verification Method (CVM) is required to complete the transaction. There are four CVM options supported by chip technology. They include Signature, Online PIN, Offline PIN, and No CVM (No Signature Required) verification.
  - Signature is the same global verification method used today when a cardholder signature is required at the point of sale.
  - Online PIN is encrypted by the PIN pad and sent "online" in real-time to the issuer host for validation. Merchants that support online PIN for mag-stripe today can continue this support for chip. Going forward, merchants that do not wish to support online PIN, do not have to support it for chip.
  - No CVM (No Signature Required) is typically used for low-value, low-risk transactions.
  - Offline PIN is sent to the chip card and is validated by the chip. An Offline PIN is never sent to the host—only the result is passed (optional).

Unlike magnetic-stripe transactions where the card does not play a role in the selection of the CVM, in chip transactions the card plays a central role. The issuer determines its preference for the CVM used for a particular transaction, which is set in the card profile in the CVM list. The CVM list on a card will have a combination of CVMs and the rules for their use.

- **Cardholder Application Selection.** Chip cards can have a single or multiple applications on a single card. Cardholders may be prompted to select which application should be used for a given transaction. Cardholder application selection only takes place when the card and terminal support more than one application in common or when required by the card. Merchants need to understand that application selection will occur on some transactions and not others and that this difference is not a problem. For example, choosing between the Visa payment application and a loyalty application.

- **Visa cards support both the Visa International (VSDC) Application Identifier and the Visa U.S. Common Debit Application Identifier.** The Visa International Application Identifier is for cross-border transactions, and can also be used for U.S. domestic transactions. The Visa U.S. Common Debit Application Identifier cannot be used for cross-border transactions. It is for U.S. Domestic transactions – Visa and those Debit networks that have agreed to support it.
- **EMV Counterfeit Liability.** Another important question is, "Who holds the liability for a point-of-sale counterfeit chip-initiated transaction?" The Visa global POS counterfeit liability shift will occur on 1 October 2015 and the ATM and AFD liability shift will be instituted in the U.S. on 1 October 2017. The liability shift only is for counterfeit cards and does not pertain to lost and stolen cards. The party that is the cause of a chip transaction not being conducted (i.e., either the issuer or the merchant's acquirer or acquirer processor) will be held financially liable for any resulting card-present counterfeit fraud losses. For information regarding liability shift requirements and timeframes for other brands, please check with your acquirer.
- **EMV Lost and Stolen Liability.** To help improve cross-border acceptance of U.S.-issued chip cards and provide a more consistent experience for cardholders, Visa revised the liability for some transactions at unattended terminals (ATMs excluded), regardless of the cardholder verification method (CVM) used. In addition, Visa requires certain unattended terminals (ATMs excluded) to allow online-authorized chip transactions without a CVM. Accordingly, the following revisions and requirements for fraud liability and terminals apply:
  - **Effective 1 April 2014**, issuers are liable for all online-authorized fraudulent chip-transactions (contact and contactless) made at an unattended terminal (ATMs excluded) that supports the processing of transactions without a CVM. In addition, all newly deployed online-capable, chip-enabled (contact and contactless) unattended terminals (ATMs excluded) that are not replacement terminals must support the processing of transactions without a CVM.
  - **Effective 1 July 2015**, all online-capable, chip-enabled (contact and contactless) unattended terminals (ATMs excluded) must support the processing of transactions without a CVM.

NOTE: While it is required to support the processing of transactions without a CVM, regular CVM processing protocol, in accordance with EMV, should be followed (i.e., if both the card and the terminal support PIN for point of sale, a PIN may be requested).

- **Fallback Transactions.** Visa policies state that chip cards must be read as chip cards at all times unless the chip card, chip reader, or terminal is malfunctioning. Chip cards may only be accepted via the magnetic-stripe when the chip cannot be read.
  - In the event that a chip card or chip reader is not functioning and the physical magnetic-stripe of the card is read, the terminal will read the service code and prompt the merchant to read the card as a chip card. Merchant staff need to understand the activities that they should perform and the sequence of events they should follow when they are processing fallback transactions. Typically, the merchant staff member will be given a number of chances to read the chip card using the terminal chip reader before the terminal prompts for fallback to be performed using the magnetic-stripe, if permitted.

- If the magnetic-stripe functionality of the card or terminal is also not working or an online authorization is not available, merchants may then fallback to existing card acceptance procedures. Fallback is allowed but should be monitored as it may indicate faulty equipment or need for staff training.
- Merchants that are in the process of enabling terminals to accept chip technology are urged to ensure that chip is enabled for all payment brands they plan to support for both the hardware and software. Terminals erroneously indicating that they are chip-enabled when only the hardware is capable are a common cause for excessive fallback which is monitored by Visa's Global Chip Fallback Monitoring Program compliance.

External Stakeholders

- Acquirer – A financial institution or merchant bank that contracts with a merchant to accept Visa cards as payment for goods and services and enables the use of Visa cards as a form of payment. Sometimes in conjunction with merchants, acquirers have a direct connection to brands/networks such as Visa.
- Acquirer Processor – A Visa-approved non-client that is directly connected to VisaNet, and provides authorization, clearing, or settlement processing services for merchants and/or Visa acquiring clients.
- Third-Party Vendors
  - POS Equipment Vendors – Select only vendors with an EMV approved device. Your acquirer or acquirer processor may have identified possible options.
  - Middleware Vendors – New middleware vendors may be required if current vendor lacks EMV expertise. Determine if existing vendors can make all identified changes.
  - Information Technology (IT) System Integration Experts – Whether outsourced or internal, these experts are a critical part of the chip implementation process when it comes to evaluating a merchant's current payment system infrastructure and incorporating the right EMV chip solution.
  - Software Application Vendors – New software application vendors may be required if the current vendor lacks EMV expertise. Determine if existing vendors can make all identified changes.

3. Building Your EMV Chip Acceptance Game Plan

Planning Is Everything

What are your merchant location EMV chip acceptance needs? What point-of-sale (POS) terminal hardware is required to meet those needs? Do you have to update your software? Which testing efforts are necessary to ensure the efficiency and accuracy of EMV chip deployment? What types of vendors are involved in EMV chip implementation?

These are just a few of the key questions you need to consider as you plan for the adoption of chip-based technologies at your merchant location(s). This section highlights 10 major steps you can take to assess the readiness of your payment system for the chip platform, and understand what's required when making a fundamental shift to chip technology. These steps are based on merchant chip implementation efforts and lessons learned in other markets where EMV chip has been successfully deployed. The timeframe for completing these steps will vary widely, depending on the size of merchant operation and Merchant Category Code (MCC).

10 Steps to Planning Full Chip Implementation

Step 1 Build Your Internal Chip Implementation Project Team

A project of this nature will most likely cross multiple disciplines within your merchant organization. With this in mind, it is important to define the roles and responsibilities for each discipline prior to starting a chip implementation project. Many of the activities have cross-discipline dependencies and successors, so it is essential that each area fully understands how it fits within the project. Merchants should be working with their acquirer and/or acquirer processor for their migration requirements.

- Identify your project team members. Your team should include business experts from the various areas in your organization that will be affected by chip implementation activities. They should be able to provide expertise for their departments and share responsibility for the project's success.
- A chip implementation project team typically includes, but is not limited to, business experts from such merchant areas as:
  - IT
  - Operations
  - Finance
  - Marketing
  - Training

  - Communication/Brand
  - Legal
  - Risk and Compliance
- **Make sure key players from areas with major project deliverables participate early in the project life cycle.** Make sure key players from areas with major project deliverables participate early in the project life cycle that may have impacts with chip processing.
- **Assign a project manager.** This person should be responsible for the overall project and project milestones. Other responsibilities include the day-to-day project management of the effort, coordination of the various groups involved, tracking of project activities and tasks, maintenance and distribution of project documentation, scheduling of meetings, and management of project issues.
- **Identify an Executive Sponsor** (if applicable in your organization).
- **If necessary, get outside consultation support.** To ensure that the project manager can focus on meeting deliverable dates and resolving issues, it may be appropriate to engage an experienced EMV chip implementation consultant to help with strategic planning efforts such as:
  - Defining project objectives and deliverables
  - Defining the project scope and estimating costs
  - Determining project timelines and tasks

Step 2 Assess Your Current Merchant Environment

To move from your current merchant payment processing environment to a desired, future state that will effectively support EMV chip contact and/or contactless acceptance, you need to conduct a strategic needs analysis. To do this, you must first assess your current operations, so that you can compare it to your future vision. To do this:

- **Document your current payment processing environment.** This allows you to identify gaps between where your merchant organization is now and where you want it to be, and determine what your team needs to strategically and tactically plan in order to close any gaps. Your documentation should include current payment data processing flow charts, system infrastructure specifications, payment decision processing points, hardware in place, software requirements, current usage extended support, financial resources available, etc.
- **Make sure current environment documentation allows for direct input from key representatives on your project implementation team.** This may include, but is not limited to the business experts referenced earlier in Step 1.
- **If applicable, include any future strategic plans that are under consideration regarding upgrades or modifications to your current environment.**

Step 3 Build Your Chip Acceptance Knowledge Base

Prepare to meet with external stakeholders, including your acquirer and/or acquirer processor, to collect the information you need to better understand what it is going to take to integrate EMV chip logic into your POS system, leverage opportunities to add new services and generate revenue, and improve customer service.

- **Schedule data collection meetings with appropriate stakeholders to obtain data necessary to update your EMV chip infrastructure.** These meetings should include your acquirer and/or acquirer processor to discuss what is necessary to upgrade your POS infrastructure to accept chip cards. Consider the below topics for discussion:
  - Chip acceptance needs (whether you'll be doing dual, contact, or contactless/mobile chip acceptance).
  - Terminal hardware options that meet your merchant organization needs, and the following components if applicable to your environment:
    - POS device – integrate, upgrade, or new installation
    - The terminal-to-merchant host interface
    - The terminal-to-merchant workstation interface
    - In-store terminal controllers
    - The merchant-to-acquirer processor host interface
    - Infrastructure of in-house back-office systems
    - Capacity planning processing, logging, and backing-up transactions
    - Terminal placement including signage, branding, and hardware installation needs
    - Software needs, including terminal and other payment related systems.
  - Determine where payments exist in your system
  - Reduce the number of touch points – isolate the payment components
  - Review current merchant testing requirements to develop acquirer recertification needs
  - Implement a Terminal Management System
  - Plan to manage deployment of dial-up terminals – more difficult to upgrade/change
  - Any reporting needs or changes
  - Resources that will be required for chip implementation
  - Changes to your customer interaction and transactional procedures
  - Determine tools that fit your testing needs by working with your acquirer and/or acquirer processor to support Visa test tools: Acquirer Device Validation Toolkit (ADVT) and Contactless Device Evaluation Toolkit (CDET)
  - Terminal deployment schedule
  - Possible live dates for each store location
  - Documentation and staff training needs
  - Ongoing support

- **Set up subsequent data collection meetings with appropriate external stakeholders.**

External Stakeholder	Possible Topics for Discussion
Acquirer	• POS devices • Terminal placement including signage, branding, and hardware installation needs • Documentation and staff training need • Any reporting needs or changes • Chip acceptance needs, whether you'll be doing dual, contact, or contactless/mobile chip acceptance
Acquirer Processor	• Merchant-to-acquirer processor host interface • Migration testing requirements
IT System Integration Experts	• Help in evaluation of current payment system infrastructure with additional requirements for incorporating the right EMV chip solution • Expected timeframe for delivery
Middleware Vendors	• Help in evaluation of any required changes in the current payment system infrastructure to support chip • Expected timeframe for delivery
POS Equipment Vendors	• Chip acceptance needs, whether you'll be doing dual, contact, or contactless/mobile chip acceptance • POS devices (Standalone or integrated) • Changes to your customer interaction and transactional procedures • Expected timeframe for delivery
Software Application Vendors	• Help in evaluation of any required changes in the current payment system application to support chip • Expected timeframe for delivery
Visa (if applicable)	• Visa participation will be at the request of the acquirer or acquirer processor with the exception of merchants directly connected to Visa. These are Merchant Direct Exchange (MDEX) merchants

Step 4 Conduct Your Merchant Needs Analysis

With the information collected from the external stakeholders, you are ready to compare your current payment processing infrastructure and requirements to those needed to support an EMV chip acceptance upgrade.

- **To ensure all business needs and requirements are met, first gather needs analysis input from key representatives on the chip implementation project team.** Each area should conduct its own internal department needs analysis to address functionality issues, preliminary requirements, and policies associated with their specific area and strategic goal.
- **Have each area representative present their findings to the entire chip implementation project team.** They need to identify the business and technical/non-technical (e.g., terminal branding, POS messaging, training, etc.) requirements they must meet, the functions/tasks they must complete, and the resources necessary to close the gap between your current payment processing environment and the future EMV chip acceptance state you wish to achieve.

Step 5 Initiate and Review Internal Plans

Once the project team has a clear picture of what's needed throughout the organization to successfully build a foundation for EMV chip implementation, it is time to begin your internal planning.

- **Schedule your internal planning meetings to build a preliminary chip implementation project roadmap that addresses the project needs.**
- **Agree upon your EMV chip implementation direction and decisions regarding system capabilities, terminal hardware and software options, organizational readiness, and system integration needs**. Map out your organization's direction, requirements, and timeline for completion.
- **Get complete buy-in from project team representatives and obtain executive sponsor approval.**
- **Prepare Request for Proposals (RFPs) for distribution to selected key stakeholders.** Each RFP should clearly specify your EMV chip implementation requirements.

Step 6 Finalize Your EMV Chip Implementation Decisions

- **Meet as a project team to finalize EMV chip implementation decisions, which can include, but are not limited to, the following:**
  - Should POS equipment be replaced?
  - Does POS software need to be upgraded or replaced?
  - What PIN pad devices are needed?
  - Which stakeholders should you partner with?

  - Which is most appropriate EMV solution:
    - Full integration?
    - Semi-integrated?
    - Standalone?
- **Review submitted proposals from potential stakeholder partners.**
- **Make decisions/recommendations and obtain internal approvals:**
  - Identify select stakeholder partners and outline their role and responsibilities.
  - Develop service level agreements.
  - Ensure all legal requirements have been met.

Step 7 Work with Selected Stakeholder Partners to Plan Your EMV Chip Implementation

- **Conduct your initial EMV chip implementation planning kick-off meeting.** It is recommended that you conduct your internal project team meeting first to make sure everyone is on board with stakeholder partners, final decisions, and agreed upon goals, objectives, and direction. This meeting should be followed by a meeting with both internal team members and external stakeholders. Discussion topics should include:
  - Project milestones
  - Estimated implementation timeline
  - Budget plans
  - Contingency plans
- **Hold subsequent implementation planning meetings that involve essential project team members and appropriate stakeholder partners (as needed).** Meeting topics should include:
  - Minimum requirements for EMV implementation such as management, systems integration, payment and retail scripts, test tools, testing and QA, PCI compliance and acquirer migration requirements
  - EMV solution maintenance requirements
  - EMV chip support requirements:
  - Help desk
  - Remote assistance
  - Monitoring
  - Annual budget planning and tracking
- **Estimate all development, hardware and deployment costs for entire project.**
  - Review submission of RFPs for new equipment (if applicable).
  - Weigh the costs and benefits and conduct a Return on Investment (ROI) analysis.
  - Ensure assessment of chargebacks and potential liability shift costs are carefully reviewed internally by the merchant/finance areas and other stakeholders where applicable.

- **Make sure all internal project team representatives are fully aware of proposed changes and approve any new modifications.** Review and get approvals for all estimated costs and estimated timeline.

Step 8 Test Your System

Visa requires that merchant terminals be tested in the merchant environment to ensure proper EMV chip functionality. There is no Visa requirement that ADVT and CDET testing be conducted for each merchant location; however, testing is required for each unique terminal configuration. Merchants should work with their acquirer and/or acquirer processor on all testing requirements for migration efforts.

NOTE: MDEX merchants should contact their Visa representative directly about testing and certification.

- **Prepare your merchant environment for EMV chip payment testing.**
  - Establish all components from PIN pad to acquirer or acquirer processor and back to merchant.
  - Ensure that all organizational areas are fully ready.
- **Begin unit test phase.**
  - Repeat testing until all components successfully pass.
  - Ensure all pertinent parties are involved.
- **Conduct string/systems testing.**
  - Repeat testing until all components successfully pass.
  - Ensure all parties are involved.
- **Start regression test phase.**
  - Repeat testing until all components successfully pass.
  - Ensure all parties are involved.
- **Begin certification test phase.** This phase will likely take the most time as it involves the acquirer processor.
  - Specified cycles are set up based on certain timing/availability.
  - Frequent communication and follow-up are essential.
  - Conduct ADVT and CDET testing. This requires the involvement of the acquirer or acquirer processor in order to set up a test environment connection into Visa's VCMS system or the acquirer processor.

Test results from ADVT and CDET testing must be entered into the *Chip Compliance Reporting Tool* by either the acquirer, acquirer processor or a Visa approved third-party chip tool supplier using the Visa Chip Vendor Enabled Service (CVES).

NOTE: Merchant Direct Exchange (DEX) merchant testing is similar to the Acquirer Processor, except it is more focused on the transaction types their business supports.

Step 9 Train Merchant Point-of-Sale Staff

- **Prepare a merchant staff training plan that includes the following tasks:**
  - Develop EMV chip transaction processing training objectives.
  - Establish training requirements.
  - Design training program specifications.
  - Develop training materials for staff trainees and support materials to assist the merchant trainers.
  - Conduct a train-the-trainer class.
- **Ensure your merchant sales staff is trained on the basic procedural differences between magnetic-stripe and chip card acceptance. Key points to cover include:**
  - **Chip cards are inserted into the chip reader and must remain inserted until the transaction is completed.** This differs from the magnetic-stripe method where the merchant swipes the card and immediately removes it in a single motion.
  - **Early removal of the chip card from the reader will terminate the transaction.** As terminal messages vary, any message that signals when a transaction is completed should be clearly identified. Merchants and their customers should be educated to remove the card from the terminal only after seeing this message.
  - **Merchant staff should prompt cardholders to insert the card into the chip reader rather than swiping the magnetic-stripe.** This will make the transaction process faster and mitigate the potential problem where an issuer may have incorrectly personalized the card with a service code that does not correspond to a chip card.
  - **Merchant staff should ensure that when the purchase is complete, the cardholder takes their card.**
  - **If a chip card or chip reader is not functioning and the physical magnetic-stripe of the card is read, the terminal will read the service code and prompt the merchant to read the card as a chip card**. Acquirers need to train merchants on the activities they should perform and the sequence of events they should follow when they are processing fallback transactions. Typically, the merchant staff member will be given a number of chances to read the chip card using the terminal chip reader before the terminal prompts for fallback to be performed using the magnetic-stripe, if permitted.
  - **If the magnetic-stripe functionality of the card or terminal is not working or an online authorization is not available, merchants may then fallback to existing card acceptance procedures.** Acquirers may need to revise their procedures on fallback related to PAN Key Entry and paper-based transactions.
  - **Ensure merchant staff members clearly understand:**
    - The application selection process and how to guide their customers in pressing the correct button(s) to select the application or account they prefer to use.
    - Cardholder verification in the chip environment. Merchants and cardholders will rely on the chip-reading terminal and the chip card to agree on which CVM is required to complete the transaction. The terminal and card interactive decision process and final selection is based on a mixture of elements that are specific to that particular transaction, such as amount, domestic or international transaction, whether the issuer's CVM preference can be met, and the other CVM options available.

- **Train your back-office personnel about chip-related chargeback issues and dispute resolution actions.**
- **Find out if your acquirer or acquirer processor will be able to assist with training. Ask them if turnkey training materials are available.**
  - Training presentation
  - Operations manual
  - Quick reference guide
  - Frequently asked questions from both the merchant and cardholder perspectives
- **Conduct follow-up training as necessary. This is especially given possible high turnover, a high incidence of fallback transactions, or both.**
- **Evaluate merchant training needs and materials regularly.**

Step 10 Perform Pilot Store Installation

- **Install required software and hardware in pilot store.**
- **Properly place contactless readers to ensure seamless usage by cardholders and maintain the principle of a fast transaction.** Some best practices include:
  - Ensure the reader is free from obstructions and easily accessible for cardholders to use the contactless payment feature.
  - Place contactless card readers at least 12 inches away from each other. In retail locations where counter space is limited, the magnetic field of multiple readers in close proximity may overlap; thus disrupting the contactless transaction when a single contactless card is presented.

Display the contactless symbol on all readers to let cardholders know how and where they can use Visa payWave cards. There are specific requirements relating to the branding of the terminals and further information can be found in the Visa Brand Mark and Contactless Symbol Guide for Payment Terminals. Visa can also provide appropriate artwork to be used for terminals and readers.

NOTE: You can conveniently select from Visa decals and point-of-sale signage from the Order Materials page on http://www.visafulfillment.com/visamerchant/main.asp.

- **Make sure all pilot store personnel have been properly trained.**
- **Educate staff about chip acceptance procedures in environments where customers insert their own cards in the chip reader.** Unattended terminals, for example, ATMs, UCATs or AFDs, should have instructional prompts and signage to support cardholders through each phase of the transaction.
- **Conduct first store pilot.**
  - Monitor results for at least 30 days.
  - Ensure acquirer or acquirer processor has approved transactions with no issues.
  - Make sure all appropriate parties are involved.
- **Document and evaluate pilot results and recommend changes for improvement.**

- **Make required changes based on pilot results and move solution to next pilot group.**
  - Implement process changes as required from first pilot store.
  - Implement software and hardware as required to next control group.
  - Ensure all appropriate parties are involved.
- **Certify pilot results and gradually roll out EMV chip acceptance using small quantities of stores.**
  - Implement software and hardware as required to required stores.
  - Continue until all stores have been fully implemented.

Appendix

EMV Chip Implementation Resources for Merchants

Visa U.S. Merchant EMV Chip Acceptance Readiness Guide Checklist

Glossary

EMV Chip Implementation Resources for Merchants

For more information about EMV chip implementation requirements, contact your acquirer or processor. The following Visa resources can be ordered directly through your Visa acquirer:

- Visa Contact and Contactless Payment Program manuals for acquirers, merchants, Direct Connect merchants, and vendors include:
  - *Visa U.S. Acquirer Implementation Guide*
  - *Transaction Acceptance Device Guide* at http://www.visa.com/tadg
  - Acquirer Visa Operating Regulation and Compliance documentation for acquirers, merchants, and Direct Connect merchants include:
  - *Visa USA, Inc. By-Laws and Operating Regulations*

To learn more about EMVCo chip payment interoperability specifications and vendor product evaluation, visit http://www.emvco.com.

To download merchant card acceptance publications, visit http://www.visa.com/merchants.

Visa U.S. Merchant EMV Chip Acceptance Readiness Checklist

Step	Actions	(🗐)	Notes
1 Build Your Internal Chip Implementation Project Team	• Identify your project team members.		
	• Make sure key players from areas with major project deliverables participate early in the project.		
	• Assign a project manager.		
	• Identify an Executive Sponsor.		
	• If necessary, get outside consultation support.		
2 Assess Your Current Merchant Environment	• Document your current payment processing environment.		
	• Make sure current environment documentation allows for direct input from key representatives on your project implementation team.		
	• If applicable, include any future strategic plans that are under consideration regarding upgrades or modifications to your current environment.		
3 Build Your Chip Acceptance Knowledge Base	• Schedule data collection meetings with appropriate stakeholders to obtain data necessary to update your EMV chip infrastructure.		
	• Set up your first data collection meeting with your acquirer and/or acquirer processor to discuss what is necessary to upgrade your POS infrastructure to accept chip cards.		
	• Set up subsequent data collection meetings with appropriate external stakeholders.		
4 Conduct Your Merchant Needs Analysis	• To ensure all business needs and requirements are met, first gather needs analysis input from key representatives on the chip implementation project team.		
	• Have each area representative present their findings to the entire chip implementation project team.		

Step	Actions	(🗐)	Notes
5 Initiate and Review Your Internal Plans	• Schedule your internal planning meetings to build a preliminary chip implementation project roadmap that addresses proposed area needs.		
	• Agree upon your EMV chip implementation direction and decisions regarding system capabilities, terminal hardware and software options, organizational readiness, and system integration needs.		
	• Get complete buy-in from project team representatives and obtain executive sponsor approval.		
	• Prepare Request for Proposals (RFPs) for distribution to selected key stakeholders.		
6 Finalize Your EMV Chip Implementation Decisions	• Meet as a project team to finalize EMV chip implementation decisions.		
	• Review submitted proposals from potential stakeholder partners.		
	• Make decisions/recommendations and obtain internal approvals.		
7 Work with Selected Stakeholder Partners to Plan Your EMV Chip Implementation	• Conduct your initial EMV chip implementation planning kick-off meeting.		
	• Hold subsequent implementation planning meetings that involve essential project team members and appropriate stakeholder partners (as needed).		
	• Estimate all development, hardware and deployment costs for entire project.		
	• Make sure all internal project team representatives are fully aware of proposed changes and approve any new modifications.		
8 Test Your System	• Prepare your merchant environment for EMV chip payment testing.		
	• Begin unit test phase.		
	• Conduct string/systems testing.		

Step	Actions	(🗐)	Notes
	• Start regression test phase.		
	• Begin certification test phase.		
9 Train Merchant Point-of-Sale Staff	• Prepare a merchant staff training plan.		
	• Ensure your merchant sales staff is trained on the basic procedural differences between magnetic-stripe and chip card acceptance.		
	• Ensure merchant staff members clearly understand: – The application selection process and how to guide their customers in pressing the correct button(s) to select the application or account they prefer to use. – Cardholder verification in the chip environment.		
	• Train your back-office personnel about chip-related chargeback issues and dispute resolution actions.		
	• Find out if your acquirer or acquirer processor will be able to assist with training.		
	• Conduct follow-up training as necessary.		
	• Evaluate merchant training needs and materials regularly.		
10 Perform Pilot Store Installation	• Install required software and hardware in pilot store.		
	• Properly place contactless readers to ensure seamless usage by cardholders and maintain the principle of a fast transaction. Some best practices include: – Ensure the reader is free from obstructions and easily accessible for cardholders to use the contactless payment feature. – Place contactless card readers at least 12 inches away from each other. In retail locations where counter space is limited, the magnetic field of multiple readers in close proximity may overlap; thus disrupting the contactless transaction when a single		

Step	Actions	(🗐)	Notes
	contactless card is presented.		
	• Display the contactless symbol on all readers to let cardholders know how and where they can use Visa payWave cards.		
	• Make sure all pilot store personnel have been properly trained.		
	• Educate staff about chip acceptance procedures in environments where customers insert their own cards in the chip reader.		
	• Conduct first store pilot.		
	• Document and evaluate pilot results and recommend changes for improvement.		
	• Make required changes based on pilot results and move solution to next pilot group.		
	• Certify pilot results and gradually roll out EMV chip acceptance using small quantities of stores.		

Glossary

Term	Description
Cardholder Verification Method	A method used to confirm the identity of a cardholder and to signify cardholder acceptance of the transaction, such as signature, online PIN, offline PIN, and No CVM (No Signature Required).
Contactless Payment	A Transaction Acceptance Device (TAD) capable of reading, communicating, and processing Visa Contactless Payment Specification (VCPS) data.
EMV (Europay, MasterCard® and Visa®)	EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point-of-sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications.
Gateways	A payment processing solution external to a merchant's card acceptance or data center environment that facilitates transaction routing to processors on a merchant's behalf.
Integrated POS	A POS system that offers card acceptance as part of a single, fully-integrated cash register system. The integrated system may include PC software, and PC and/or terminal hardware components.
MDEX (Merchant Direct Exchange)	A merchant directly connected to Visa without passing transaction data through an acquirer processor.
Middleware	A third-party software solution used in conjunction with a separate POS system. Typically middleware complements a cash register system that does not offer its own card acceptance and processing capabilities.
Payment Card Industry (PCI) Data Security Standard (DSS)	A comprehensive set of international security requirements for protecting cardholder data. The PCI DSS was developed by Visa and the founding payment brands of the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis.
Stand-Alone Terminals	A stand-alone terminal typically sits on a merchant's countertop or is mounted to the wall. These terminals are not integrated with other systems in the merchant card acceptance environment.
Switches	A switch is a hosted software solution, typically resident in a merchant's central data center, used to route transactions across multiple channels.