BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

Fiscal Service Government-wide Implementation of EMV Chip & PIN at the Point-of-Sale

Frequently Asked Questions

[Updated 5/11/2015]

What is EMV?

EMV is a series of specifications defining a more secure method of card payment developed jointly by Europay, MasterCard, and Visa in the mid-1990s. EMV's goal is to facilitate secure global interoperability between chip cards and terminals for credit and debit card transactions.

- EMV introduces a small computer or "chip" to every card or other payments device. This computer chip stores information, performs processing, contains secure elements that store secret information, and performs cryptographic functions.
- Chip & PIN card acceptance at the point-of-sale (POS) involves the cardholder inserting the payment card into a reader (as opposed to swiping) and entering their unique code on a PIN pad.
- The most important feature of EMV is the dynamic data generated with each transaction. This dynamic data makes it nearly impossible to create counterfeit cards or replay intercepted transactions.

Why is the Fiscal Service asking federal agencies to deploy EMV-enabled chip & PIN terminals?

Executive Order 13681 requires executive departments and agencies to transition payment processing terminals and credit, debit and other payment cards to employ enhanced security features – specifically Europay MasterCard Visa ("EMV") "chip & PIN" technology.

- All new payment card terminals acquired through Treasury or through alternative means authorized by Treasury after December 31, 2014 must include hardware to support EMV chip & PIN ("EMV-capable").
- For existing card processing terminals acquired through Treasury, a plan must be in place by January 1, 2015 for agencies to install software necessary to enable EMV chip & PIN acceptance ("EMV-enabled").

Adoption of EMV chip & PIN at the point-of-sale significantly reduces exposure to counterfeit card use. To comply with the Executive Order and set the standard for POS card acceptance in the U.S., the Fiscal Service's Card Acquiring Service (CAS) is working with its agencies to deploy EMV-enabled terminals as replacement for existing non-compliant standalone terminals by no later than September 30, 2015.

Where can we purchase replacement terminals? Who will be paying for the terminals?
It is important here to recall that there are two Federal agency POS card acceptance environments supported by CAS: (1) standalone terminals acquired through CAS; and (2) third-party provisioned integrated POS systems employed at some CAS customer agencies. Let's apply this question to each scenario:

1. Pursuant to the plan called for by the Executive Order to replace terminals acquired through Treasury, The Fiscal Service is bulk purchasing EMV-enabled terminals (including wireless where necessary) and PIN pads to replace existing agency standalone terminals that are not already EMV-capable. For EMV-capable standalone terminals already deployed, the Fiscal Service is purchasing PIN pads and will make EMV-enabling software available to download. These terminal/PIN pad combinations (or alternatively EMV software and PIN pad) are being made available to CAS customer agencies as replacements for active, non-compliant terminals. To transfer terminal ownership to the agency and to authorize agency reimbursement of the Fiscal Service for its replacement equipment and related deployment costs, each agency will receive and be asked to execute an inter-agency agreement (IAA) with the Fiscal Service under the Economy Act.

2. For all other environments (i.e., integrated POS or computer-based integrated solutions), agencies should be developing their plans to comply with the Executive Order's requirement for all new (i.e., post 12/31/2014) POS card acceptance hardware purchases to be EMV-compliant. Agencies also need to be mindful of the shift in liability, as of October 1, 2015, to the agency for counterfeit card use at the POS under card brand rules if it is not EMV-compliant. Your plan should include: working with your solution provider to identify any hardware and/or software changes that will be necessary; when these will become available; and will they be certified as EMV-compliant by the card brands. System upgrades will also need to be compatible with Vantiv processing. Please talk with your Chief Counsel Office to determine the applicability of the EMV order to your agency.

Does our agency need to return a completed interagency agreement before we can schedule replacement terminal deployment?
No, while the Fiscal Service expects to be reimbursed for actual standalone terminals delivered to your agency (and related costs), a completed IAA is not necessary as a prerequisite for terminal deployment. The most immediate need is for your agency to review the "Configuration Summary" (CAS' list of standalone terminals currently registered to your agency) sent to you in advance and

respond with validation of (a) which terminals you intend to replace, and (b) which terminals, if any, are inactive and should not be replaced. We understand that a completed IAA will likely follow a separate and potentially longer review and approval process at your agency.

A. EMV-Compliant Standalone Terminals:

How will Fiscal Service-provided replacement terminals be configured?
The full replacement suite will be the Ingenico iCT220 terminals and iPP310 PIN pad as a one-for-one terminal replacement combination. This combination will be EMV chip & PIN-enabled, supporting both credit and debit card acceptance (including traditional mag stripe swipe cards and PIN debit) and Near Field Communications (NFC) authorization. Agencies that already possess EMV-capable Ingenico or Verifone terminals will receive downloadable EMV-enabling software and a compatible PIN pad to become chip & PIN enabled. Agencies with wireless terminals will receive downloadable EMV-enabling software or a replacement wireless terminal as applicable

Will we need to replace the whole terminal?
If it is a standalone terminal that is not already EMV-capable and supported by CAS (i.e., Verifone Vx520, Ingenico iCT220, or Ingenico iCT250), the terminal(s) will need to be replaced. Terminals can be purchased through Vantiv or any source but currently only the three models previously mentioned will support EMV through the CAS program. Further, if you have any of the EMV-capable terminal types but no PIN pads, you will need to acquire these to become fully chip & PIN-capable. If your customers swipe their own cards to initiate a transaction on a device that is not readily available (i.e. behind a counter or partition), you may need to purchase an additional PIN pad. As noted above, Treasury's plan includes the acquisition of EMV-enabled terminals and PIN pad combinations for deployment to agencies. If you already have EMV-capable standalone terminals, you will need the EMV-enabling software download and the PIN pad to meet the necessary chip & PIN capability. CAS will make these available to you.

Will replacement terminals include Near Field Communication (NFC) capability? Since the executive order has mandated the use of chip and PIN, what is the value of NFC capability in a device? Please clarify when/if it would be appropriate to use NFC.
NFC capability allows for contactless payment solutions where a properly configured device that is near the terminal can initiate and authorize the transaction without actually having to touch the terminal. However, please note that not all NFC form factors necessarily support EMV standards, just like some plastic cards will support EMV while others will not. Further, this is a dynamic area with recent NFC technologies introduced to the marketplace or announced.

What happens to our old standalone terminals once replaced with EMV-compliant terminals?
Terminals that are replaced will be deactivated and no longer functional. The agency does not have to do anything specific in this regard other than remove the terminals from service. Some

older terminals may retain sensitive data and agencies should dispose of all deactivated terminals properly, following their agency's policies for the destruction and disposal of electronic equipment.

Our agency recently purchased Verifone 805 terminals as a part of our integrated POS solution. Will we need to purchase replacement terminals or will Treasury provide them?
At this time, integrated POS solutions and their associated terminals (Verifone 805 or otherwise) are not part of the potential pool of replacement terminals. See the FAQ above regarding the need to engage your solution provider.

If I am in a location outside of the United States, how will I obtain a replacement terminal?
For locations outside of the United States, you should identify to CAS a stateside point of contact and address to receive your initial terminal shipment. This point of contact would assume responsibility for shipping the terminal to your final destination. Once located in your final destination, we will work with you through your stateside contact to install the replacement terminal.

What is the cost for the standard EMV terminal and pin pad?
An EMV-compliant and NFC-enabled terminal/PIN pad combination will cost agencies $314 apiece. PIN pads alone (for upgrading existing EMV-capable terminals) will cost $170. Handling will be at cost of $8.32 per order and shipping is pass-through to the agency, but is estimated at $8.00 - $15.00 per terminal, and professional fees for installation support are $73 per Merchant ID. Many customer agencies only have one Merchant ID, while others have multiples depending on the scope of their operations. Merchant IDs are often synonymous with each site at which an agency operates POS card terminals.

B. Non-Standalone Terminals/Agencies with Integrated Solutions:

Should our agency wait for Treasury to release their plan before we define our own plan?
For standalone terminals supported by the CAS program and its acquirer Vantiv, agencies should work directly with the Fiscal Service, since it is acquiring EMV-compliant terminals with compatible PIN pads in bulk for deployment to CAS customer agencies under Treasury's plan. For non-standalone POS environments (i.e., integrated computer-based POS solutions), agencies should be developing plans to comply with the Executive Order's requirement for all new POS card acceptance hardware purchases to be EMV-compliant. Agencies employing integrated POS solutions should also be mindful of the October 1, 2015 shift in liability to the merchant/agency for counterfeit card use under card network rules and be prepared to accept this liability of integrated POS card acceptance points are not EMV-compliant by that date. Please talk with your Chief Counsel Office to determine the applicability of the EMV order to your agency.

Since agencies with integrated POS systems do interface with CAS for processing, we would appreciate such agencies sharing their planning with us. Agency compliance plans or summaries can be sent to **EMV@fiscal.treasury.gov**. Please enter **"[AGENCY NAME] ISV EMV Compliance Plan"** in the subject line.

Should plans for EMV through non-standalone sources come from the agency or at the program or other level (i.e. Army Corps of Engineers, Recreation.gov, or Department of Interior)?
Each agency, program, or specific entity that processes transactions through the CAS program should determine the best approach from its perspective to address the Executive Order and its underlying mandate for EMV.

Can Treasury grant an agency a waiver if they are not EMV compliant by September 30?
Treasury is not in the position to grant waivers. Our plan embraces deploying replacement EMV-enabled terminals and PIN pads to agencies that currently possess non-compliant standalone terminals acquired through the program. As noted, we intend to accomplish this no later than September 30th and are working with each customer agency to identify terminals to be replaced, to be upgraded, or to be deactivated. Agencies will agree to reimburse Treasury/Fiscal Service for the cost of replacement terminals and/or upgrades. For agencies with their own integrated commerce systems that have point-of-sale card acceptance points (which go by many names including VARs, ISVs, etc.), the EO requires that any upgrades to card acceptance capabilities acquired after 12/31/2014 be EMV-enabled. Therefore, agencies with such solutions should be talking to their providers about their EMV upgrade capabilities and considering upgrade planning.

Again, as customers of the Card Acquiring Service, Treasury/Fiscal Service would like to be informed of each agency's planning, in summary form at least, on a go-forward basis. Plans or their summaries can be sent to: **EMV@fiscal.treasury.gov** with "**[AGENCY NAME] ISV EMV Compliance Plan**" in the subject line.

C. Card Not Present Scenarios:

Our agency's card processing environment is primarily Pay.gov and telephone-based transactions, with one terminal used for customers who do not access Pay.gov. Will EMV apply in this environment?
Currently EMV supports only terminal-based, "card-present" transactions at the point-of-sale. At this time, there is no need to do anything differently for "card-not-present" transactions. Any terminal that the card holder accesses at the point-of-sale is a terminal that will need to be able to process EMV chip & PIN transactions. Therefore it would need to be replaced. Further, if a terminal is operated by agency personnel entering card transactions from customers received via the web, telephone or other card-not-present means, then we also recommend you obtain a replacement EMV-enabled terminal to ensure compliance with the chip & PIN standard if you ever

choose to repurpose this terminal to accept card-present transactions. Otherwise, your process does not need to change and no new hardware or software is required.

Can you please clarify the details of EMV for card-not-present transactions?
EMV does not apply in the non-POS CNP environment since there is no physical presence of an actual card.

D. Other:

As of the liability shift that occurs October 1, 2015, if a customer wants to swipe their card the old way because they do not have a new chip card, are we required to reject the transaction? Can you clarify when/if it would be appropriate to continue to use magnetic swipe?
All replacement terminals will retain swipe capability for people who do not have EMV chip cards and their only way to conduct transactions is through a swipe of their card. If a customer does have a chip card and swipes it at an EMV-enabled terminal, the terminal will prompt the customer to insert the card in the card reader to be read.

After September 30, the liability will shift to the merchant for fraudulent transactions if the merchant is not EMV compliant. Today, which entity is responsible for fraudulent charges?
The card issuing bank is responsible today for all counterfeit liability on swiped or imprinted sales. As of 10/1/2015, under card rules, the merchant (or agency in our case) will be responsible for counterfeit card use if an EMV card is presented and they do process the EMV chip at the point of sale (i.e., card present only) and will bear this liability through the chargeback of the transaction. See shift in liability illustrated here.

With an EMV compliant terminal, if a card is rejected, will the agency know why it was rejected/declined?
Yes, this should not be any different than card rejection at the POS today with traditional swipe.

Is there an EMV impact to POS transactions authorized online (vs. offline) and what does that process look like?
By the very nature of the chip card reading process, POS EMV transactions can take several seconds longer than traditional card swipe transactions, but otherwise operate in the same way. If a chip card is swiped, the terminal will prompt the card holder to insert the card in the card reading slot. Once inserted, the chip card must remain in the slot to be read and to proceed with the transactions. The cardholder will be prompted to enter their PIN if one is associated with the card and the necessary PIN pad is included with the terminal. This same process holds true regardless of whether POS authorization is online or offline.

Did Treasury receive funding with the EMV Executive Order?

Treasury did not receive funding for payment card acquiring compliance through the EO. For standalone terminal replacement under the Treasury's plan, we are acquiring compliant terminals and compatible PIN pad combinations in bulk for deployment to our agencies, with reimbursement expected from each agency. We are working with each agency to identify their specific replacement terminal needs so that they acquire only the number of terminals they require.

HAVE A QUESTION NOT ANSWERED ABOVE? SEND IT TO EMV@fiscal.treasury.gov