Consumer Device Cardholder Verification Method

What is Consumer Device Cardholder Verification Method?

Consumer Device Cardholder Verification Method (CDCVM) is a type of Cardholder Verification supported by the card networks when accepting contactless transactions originating from mobile devices. Cardholder verification is used to evaluate whether the person presenting the card is a legitimate cardholder and affects where the liability lies for fraudulent transactions.

With Apple Pay, Touch ID or the device passcode can be used as the consumer device verification method, instead of the more traditional methods of PIN or signature.

For Apple Pay EMV transactions, CDCVM is performed and verified entirely on the iOS device (i.e. iPhone 6 and Apple Watch). During the transaction, no additional customer action is required on the payment terminal or paper receipt to verify the customer, such as a signature or PIN.

Why should a merchant support CDCVM?

- **Reduced chargeback related costs** — Merchants will not carry liability for chargebacks when CDCVM is obtained for Apple Pay EMV transactions. As a result, a merchant's bottom line improves through chargeback reduction and reduced back-office handling of signature documents.
- **Faster throughput** — CDCVM transactions allow the merchant to gain faster throughput at the register. Merchants will no longer be required to prompt for customer signature or PIN for any Apple Pay EMV transactions with CDCVM — this includes signatures for EMV transactions.
- **Increased customer satisfaction** — Customers will experience a more convenient and seamless transaction inside your locations. Cashiers will no longer need to ask to verify signature against government issued IDs.

Who should support CDCVM?

CDCVM is applicable for any merchants accepting contactless transactions originating from mobile devices. CDCVM appeals to merchants who are in high foot traffic locations, operate in a high-transaction industry, care about speed and throughput at the register, or have high incidences of no-signature chargebacks.

Some applicable industries are:
- Retail and all sub-categories
- Grocery

- Drug Store
- Casual / Full Fare Dining
- Professional Services (e.g. hair salons, doctors, dentists, independent pharmacists)
- Hotels
- Movie Theaters
- Convenience Stores
- Sporting Venues

How does CDCVM work?

CDCVM is a method to verify the cardholder of a payment transaction. The full list of supported verification methods for a contactless EMV transaction is:

1. Online PIN
2. CDCVM
3. Signature
4. No cardholder verification method

For each EMV transaction, the payment terminal and the supporting Network applications within the iOS device must mutually decide which cardholder verification method to use. In order to make this decision, both the terminal and the iOS device store a list of above verification methods that each support. The first method that is supported by both terminal and iOS device is selected as the verification method.

For Apple Pay transactions, CDCVM acts in place of PIN or signature verification when it's supported by the payment terminal.

During the authorization request, the cardholder verification method used is passed from the payment terminal to the issuer. The verification method is then used to determine fraud liability based on card network policy.

What contactless specs support CDCVM?

The major card networks support CDCVM as part of their contactless specifications. Each card network has a different contactless spec, of which installation is required to support contactless payments using the given network.

Visa supports CDCVM in their VCPS spec 2.1 and later or any version of EMV Contactless Kernel 3. Visa supports CDCVM for both credit and debit EMV transactions routed through VisaNet.

MasterCard supports CDCVM in their PayPass spec 3.0 and later for credit and debit EMV transactions. Note, MasterCard uses the terminology On-Device CVM (ODCVM). MasterCard supports CDCVM for both credit and debit EMV transactions routed through the MasterCard network.

American Express supports CDCVM for Apple Pay mobile contactless transactions in their ExpressPay terminal spec 3.0 and later.

Do card issuers still bear liability for CDCVM transactions?

The Card networks mandate where liability lies for fraudulent transactions based on criteria including how the customer was verified during the transaction.

Visa assigns liability to the Issuer for EMV transactions performed with CDCVM on terminals compliant to VCPS 2.1 and later or EMV Contactless Kernel 3.

MasterCard shifts liability to the Issuer for EMV transactions performed with CDCVM on terminals compliant to PayWave 3.0 or later.

American Express intends to shift liability to issuers for EMV-mode and mag-stripe Apple Pay mobile contactless transactions performed with CDCVM. Please refer to applicable American Express policies. Note that merchant-specific policy for CDCVM will be released in October 2015.

What do merchants need to do?

Merchants need to validate that both their payment terminals and acquirer support CDCVM for EMV transactions.

1. The merchant's payment terminals must support the required contactless specifications provided by the card networks, versions specified above. For example, the terminal must support PayPass spec 3.0 or later for MasterCard EMV transactions and VCPS 2.1 or later for Visa EMV transactions.

2. The merchant's payment terminals must be configured to accept CDCVM as a verification method. Each payment network's configuration is slightly different. The contactless specification for each will specify the exact configuration required.

3. Finally, the merchant's acquirer must support CDCVM, and the merchant must configure the CDCVM capability with their acquirer. This is typically done through an implementation statement between a merchant and their acquirer. Please consult your acquirer directly for more information.

How does CDCVM differ from floor limits?

Card Networks typically set a Reader Cardholder Verification Method (CVM) Limit in which transaction amounts above this limit require cardholder verification. Transactions under this limit require no cardholder verification while still maintaining issuer liability.

CDCVM is not to be confused with the Reader Cardholder Verification Method limit in which no cardholder verification is required for low ticket transactions. As CDCVM is a fully valid cardholder verification method, CDCVM is supported for all transactions.

Is CDCVM supported for PIN Debit Networks?

No. When routing transactions over PIN Debit networks (i.e. for Durbin), CDCVM is not a supported verification method. Customers will need to enter their PIN on the payment terminal, as they do today.