verifone

Preventing EMV Offline Contactless Fraud

How to assess your environment and implement best practices.

www.verifone.com

Executive Summary

EMV Offline Contactless Fraud.

Retailers, especially in the United States and Canada, have experienced a sophisticated fraud attack using the EMV Offline Contactless transaction method.

Method of Fraud.

The fraud actors used a mobile digital wallet with a credit or debit card on an Android device to emulate an offline approved contactless transaction.

Typical EMV Offline Contactless Use.

EMV Offline Contactless transactions are mostly used in specific industry such as transit to support low-value transactions in high-traffic environments without sending the authorization to the card issuer.

Review of Payment Environments.

Providers and operators of merchant payment systems, including point of sale software solution providers, payment terminal providers, payment application providers, payment gateway providers, acquiring hosts and merchants need to review how EMV Offline Contactless transactions are being processed in their environments. Fraud actors are exploiting how EMV Offline Contactless transactions are treated and processed in the processing ecosystem to conduct fraud.

verifone

Best Practices to Prevent Fraud.

Verifone recommends following the EMV Offline Contactless specifications and EMV kernel recommendations to detect anomalies in contactless transactions, review how such transactions are treated in current implementations and to detect vulnerabilities. The purpose of this whitepaper is to provide information about the threat, guidance on reviewing implementations and help providers and operators of payment systems ensure appropriate checks are in place in the payment environment.

Audience.

This whitepaper is intended for businesses and entities that provide and operate payment systems, including merchants, point of sale software providers, payment terminal providers, payment application developers, payment gateways providers and acquiring hosts who play a critical role in processing these transactions.

Introduction

With the recent fraudulent transaction attacks conducted using the EMV Offline Contactless method, especially in the United States and Canada retail environments, Verifone has been working diligently with several retail clients and partners across the ecosystem, including POS software providers, payment gateway providers and acquirer processors, to identify the types of fraud scenarios perpetrated and potential vulnerabilities in payment environments. This whitepaper explores the fraud risks associated with EMV Offline Contactless payments and highlights the various strategies and technologies available to prevent such fraud. Methods such as employing cryptographic protections and setting transaction limits are available to safeguard merchants while ensuring that contactless payments remain a secure and efficient option – even offline.

verifone

EMV Contactless Interaction at Payment Terminal

The EMV kernel in the payment terminal interacts with the contactless card or wallet. It examines a variety of data elements, both from the card and the merchant environment and sets the respective indicators that inform the calling application to decide and take the next action.

The following diagram illustrates the interaction between various components when a contactless wallet with a credit or debit card is presented in a merchant environment to a payment terminal.

Contactless Wallet: A credit or debit card is added to a mobile contactless wallet. In a typical scenario, cardholders add their card in a mobile wallet supported by the Issuer to participate in the wallet. There are various examples of wallets, such as Apple Pay and Google Pay, which support the secure and tokenized addition of the cards.

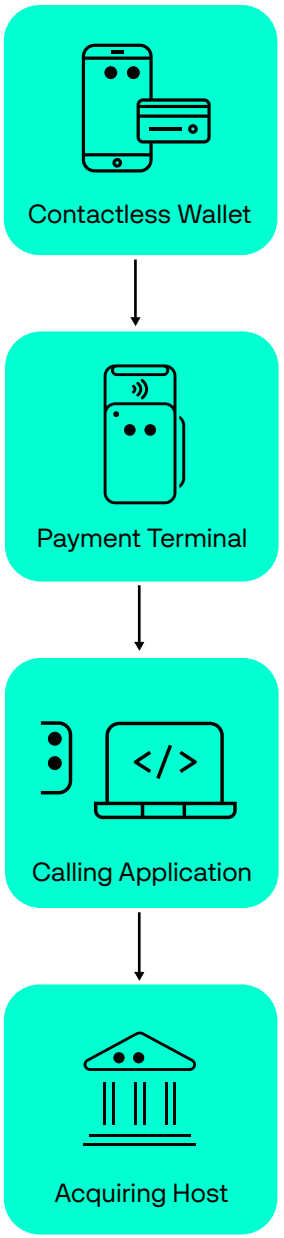
Payment Terminal: An EMV certified payment terminal interacts with the contactless wallet, exchanging information with the card in the wallet through NFC and determining if the card information received should proceed to the next step. The kernel in the payment terminal performs further checks pursuant to the EMV specifications and can either decline the transaction (offline decline), approve it offline, or send it for online approval. The software kernel presents the card information and its determination whether to send the transaction further to the calling application.

Calling Application: This is typically payment application within the payment terminal or a point-of-sale application on a POS system that interfaces with the terminal and receives the EMV card data. The role of the calling application is to evaluate the transaction data read by the payment terminal, including the EMV card data, and to determine whether to send the transaction to the issuer to request approval. The calling application should adhere to the specifications published by the acquiring host so that the message can be sent in the appropriate format to process the transaction. The calling application must take the EMV kernel's indication to either decline the transaction or send the transaction online to the acquiring host for an approval request.

In non-direct-to-host implementations, the calling application will send this data to a point of sale provider or a payment gateway provider, which will, in turn, send it to an acquiring host.

Acquiring Host: The acquiring host processes transactions and routes them for approval to the network and the card issuer based on the message type. The acquiring host may also apply its own fraud monitoring steps and rules to determine whether a transaction should proceed or be declined.

Typical transaction interaction between the components:



verifone

Fraud Vectors in EMV Offline Contactless Transactions

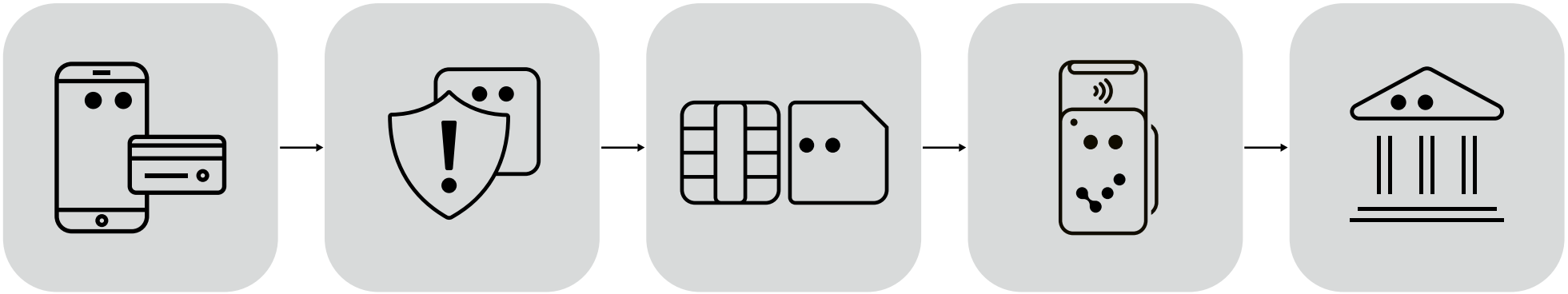
Fraud actors continue to become more sophisticated and use various methods to attempt fraudulent transactions. These fraud tactics continue to evolve and create new threats that the payment ecosystem continues to identify and build defenses against. The following are some of the general methods that are attempted for offline contactless transactions:

- **Lost/Stolen Cards:** Offline transactions may allow fraud actors to use lost or stolen cards circumventing blocks placed on them by the issuer.
- **Replay Attacks:** A fraud actor may capture valid EMV data through NFC and replay that data as an offline transaction and attempt for offline approval.
- **Improper Card Emulation:** Fraud actors may use smartphones or other devices to improperly emulate a card and initiate transactions with offline approval.

The latest fraud attempts becoming more prevalent recently are using a card added to a fake wallet on a smartphone and emulating an offline contactless transaction. It is also important to note that fraud actors may add multiple branded cards (Visa, Mastercard and AMEX) under a single AID to attempt an offline contactless transaction to exploit specific behavior and EMV implementation of each payment network.

verifone

How Fraud Actors Emulate Offline Transactions with a Fake Wallet



Fraud actors employ a malicious mobile application, a “Fake Wallet” (not associated with a valid wallet provider such as Apple, Google, or Samsung) to conduct fraudulent transactions.

The Fake Wallet application allows malicious actors to execute contactless transactions by fraudulently imitating offline eligibility through the EMV protocol to convince payment components in the flow to force offline transaction approval.

Even when an EMV kernel determines that a transaction should be processed online and therefore requests an online cryptogram from the card, these Fake Wallets send data elements through Near Field Communication (NFC) that is indicative of the card responding with “offline approval” data.

When the Fake Wallet value indicates an offline approval, there is a conflict between the kernel’s recommendation to go online and the card’s decision to approve offline. Such a conflict may mislead the calling application and other components into believing that the transaction can be processed without real-time authorization from the card issuer.

A failure to force a transaction online in the case of a conflict can occur in any of the following components depending on the implementation:

- Payment application on the payment terminal
- POS system for integrated payment systems
- Gateway/processing systems; or
- Acquiring host systems.

verifone

How Fraud Actors Emulate Offline Transactions with a Fake Wallet

The following contactless transaction scenarios illustrate what may result from different sets of conditions and the interactions of the card, payment terminal, calling application and acquiring host.

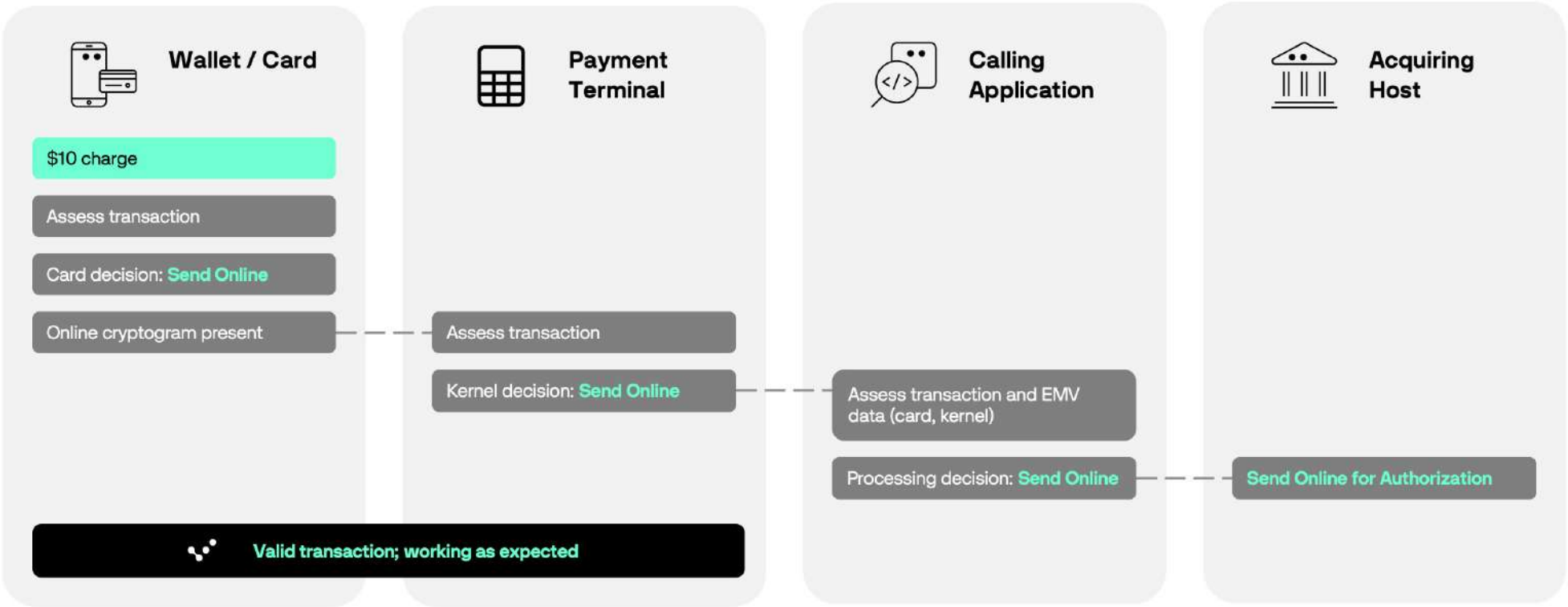
- Contactless Transaction with no offline support with a valid card in wallet
- Offline Contactless Transaction with a valid card in wallet
- Contactless Transaction with no offline support with an invalid card in wallet

Please note, that scenario 3 presents the potential fraudulent scenario where the card is provisioned in a fake wallet emulating an offline approved transaction.

verifone

Scenario 1: Contactless transaction with no offline support with a valid card in wallet

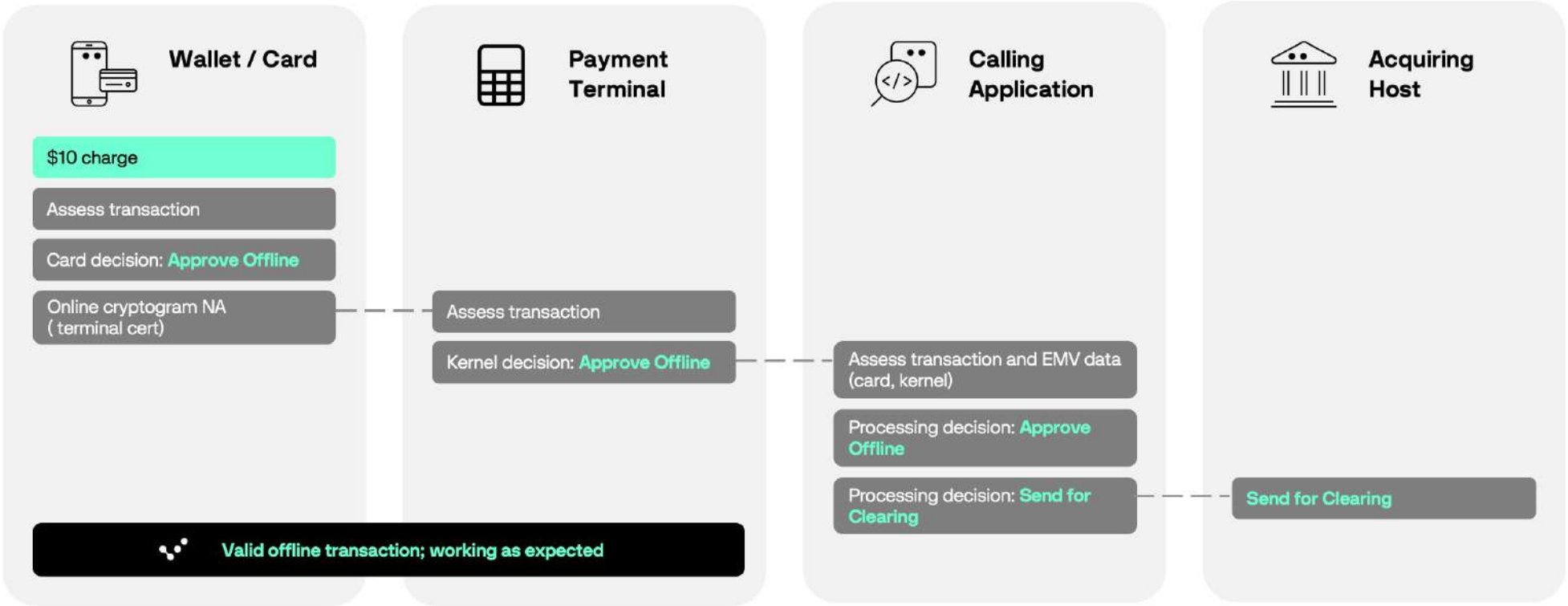
Contactless Floor Limit Value: $0



verifone

Scenario 2: Offline contactless transaction with a valid card in wallet

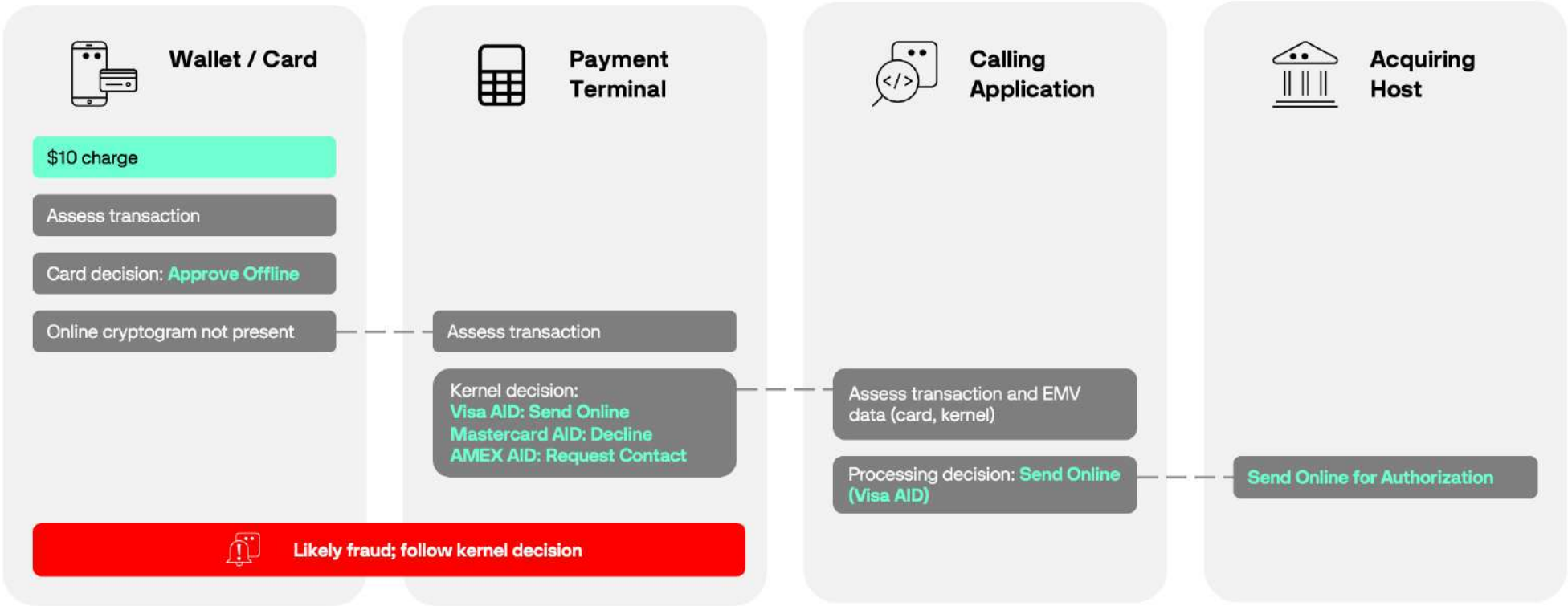
Contactless Floor Limit Value: $20



verifone

Scenario 3: Contactless transaction with no offline support with an invalid card in wallet

Contactless Floor Limit Value: $0



verifone

Best Practices to Detect and Avoid EMV Offline Contactless Fraud

Merchants and service providers should verify their payment environments and their implementations to ensure they follow best practices to avoid exposure to and prevent sophisticated EMV Offline Contactless fraud attacks.

Due to the confidential nature of the EMV contactless specification, this whitepaper does not refer to the individual data elements, conditions and values. If you are a Verifone customer or use any of our products or services, please contact a Verifone representative for further information, and Verifone can help you review your implementation.

Contactless Floor Limit

Merchants can configure and control their choice to support EMV Offline Contactless transactions using a specific floor limit configuration that payment terminals will apply when a contactless card is presented.

If the merchant does not intend to accept offline contactless transactions, it should work with its service providers to ensure the contactless floor limit is set to $0. With a floor limit of $0, if any fraudulent card is presented for any monetary value greater than $0, the transaction cannot be approved offline.

Merchants who want to enable EMV Offline Contactless transactions up to certain amounts can do so by setting and managing the specific floor limit.

Enforcing the Kernel's Recommendation

The kernel in the payment terminal is designed to assesses the input parameters, including what information the card presents, and set the recommendation pursuant to EMV specifications. The kernel in the payment terminal is always tested and certified to meet the specification. The payment terminal presents this information to the calling application to process the request further. Whenever there is a conflict between the card and the kernel's recommendations, the calling application should strictly follow the kernel's recommendation. The following are the key EMV data definitions that must be taken into consideration when assessing your environment.

Cryptogram Information Data

This represents the indicator set by the card in the contactless wallet for offline approval. A properly provisioned card will present for offline approval only when the conditions are met where the contactless floor limit is set to a non-zero value to allow offline transactions.

Terminal Transaction Qualifiers

The EMV kernel for each of the payment network sets the corresponding value indicating its recommendation —based on its assessment of the transaction. Please note the EMV tags could be different for each of the payment network pursuant to the EMV specification.

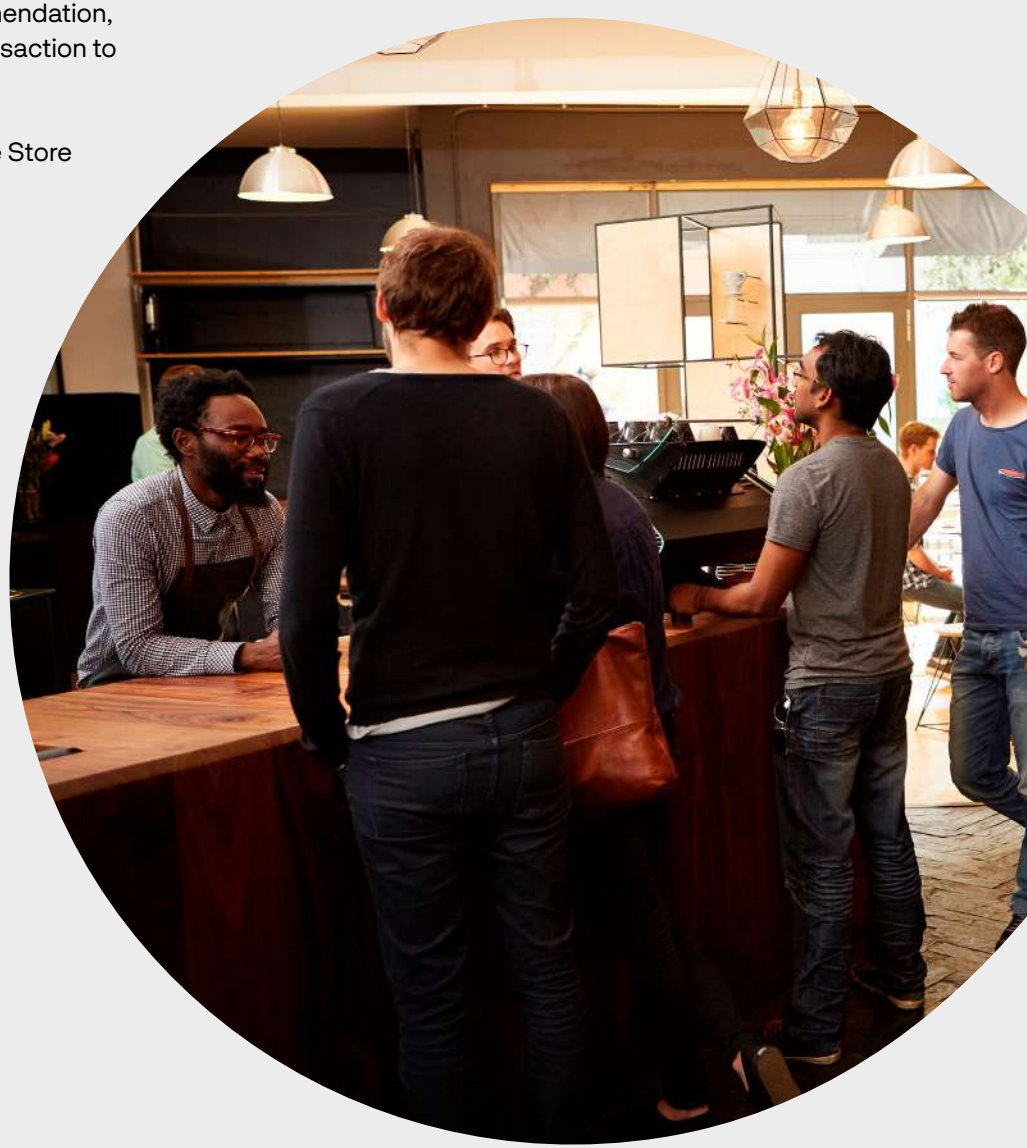
verifone

Handling Store and Forward Transactions

Some merchants may prefer to allow transactions to be approved under a certain value if their payment system cannot connect online for real-time authorization. Merchants can set a separate transaction limit for this 'Store and Forward' capability. The calling application should assess and evaluate the transaction including card's recommendation, kernel recommendation, transaction amount and contactless floor limit values before deciding to allow the transaction to be stored and forwarded due to system availability.

Let us consider the following example in a merchant environment that has enabled the Store and Forward option.

Contactless Floor Limit	$0
Store and Forward (SAF) Transaction Limit	$100
Transaction Amount	$15
Expected Card's Recommendation	Send Online
Actual Card's Recommendation	Approve Online
Kernel Recommendation	Send Online
Connectivity to Host System	Offline (no connectivity)
Calling Application's Recommended Action	Decline Transaction
Processing Note	While this transaction may have been allowed in a typical scenario since the transaction amount is within the SAF limit, given the conflict between card and kernel recommendation for offline transaction, as a best practice, the calling application should decline this transaction, when there is no connectivity to the host system for online approval.



verifone

Conclusion

Businesses and entities that provide and operate payment systems, including merchants, point of sale software providers, payment terminal providers, payment application developers, payment gateways providers and acquiring hosts should review their current implementations to detect and address any vulnerabilities.

At Verifone, we take external fraud attempts very seriously and have taken immediate steps to identify and prevent the risk of fraud exposure to our customers.

verifone

Verifone
817 Broadway, Suite 1100
New York, NY
10003, USA
Phone: 1-800-VERIFONE

www.verifone.com

Omni-Commerce Solutions for
Powerful Customer Experiences

verifone