Merchant Processing During Communications Disruptions

Version 1.0 – April 2016

This white paper discusses best practices for merchants processing EMV chip transactions during communications disruptions. The scope of this document is limited to merchant processing during communication disruptions and does not address situations when the issuer host is offline or where a network performs stand-in processing on behalf of the issuer. Issuer offline support needs should be addressed with the card issuing network(s). This document is limited to outages as seen at or by the merchant, not at the network or gateway level.

When a merchant has a communication disruption, several options exist for continuing to process transactions so as not to impede commerce. These options carry varying risks to the merchant, and require different systematic implementations. The three processing options discussed below include:

- EMV offline authorization
- Deferred authorization of an EMV card transaction
- Force post of an EMV card transaction

Voice authorization during a communication disruption for both merchant and issuer referral does not change with EMV.

Guidance in this white paper is limited to payment networks that participated in the review of this document.[1] Merchants should discuss processing transactions when communication is interrupted with their acquiring processor(s) and various networks involved in the processing of payment transactions.

This document assumes an understanding of EMV chip transactions and data elements. For additional information on EMV chip transactions and the terms used in this guidance, please refer to the EMV specifications.[2]

EMV Offline Authorization

Definition: An offline EMV authorization is a transaction resulting from request by the terminal to the chip card for approval (TC) of a transaction without requesting a real-time online authorization of the transaction from the issuer host. The card and merchant terminal must support (and be certified for) offline authorization in order for an offline authorization of an EMV payment transaction to occur.

In an online-preferring environment, if both an EMV card and EMV terminal are offline-capable, they are likely only to engage in requesting and receiving offline authorization if the terminal was unsuccessful in

[1] Networks included Accel, AFFN, American Express, Discover, FIS/NYCE, MasterCard, PULSE, SHAZAM, STAR and Visa.

[2] http://www.emvco.com/specifications.aspx?id=223.

receiving an online response from the issuer host. Note: the U.S. is an online-preferring market and this document only addresses online-preferring terminals.

In the scenario where online connectivity is temporarily not available, it is possible for the terminal to use the second Generate AC to ask the chip to approve the transaction. The chip can respond with either a Transaction Certificate (TC) as approval of the transaction or respond with an Application Authentication Cryptogram (AAC) and indicate that it is declining the transaction. When the online authorization request is processed after the first Generate AC is completed and the terminal is unable to go online, the second Generate AC process between the terminal and card will be used to determine if the transaction is approved or not based on the applicable merchant (terminal) floor limits and issuer (card) offline risk parameters. If the transaction amount is below both limits, it may be approved offline and the card generates the TC. If the amount is above the terminal, network or issuer floor limit, the terminal should request an offline decline and optionally revert to deferred authorization processing. Best practices for risk management should be considered as part of the approval process.

The U.S. Common Debit AID is online only and out of scope for this EMV offline authorization section.[3]

Clearing (Dual-Message): If offline approved, the transaction, including all EMV data as identified by the networks, must be provided in the clearing record. Offline EMV authorization declines (AAC) should not be submitted for clearing, but the original transaction information can be held for a deferred authorization attempt, or the information could be force posted (see merchant implications). Please refer to the next section, Deferred Authorization, for guidance on this process. ***Please note:*** U.S. debit payment networks do not support batch clearing.

Liability: Since an authentic EMV transaction occurred, counterfeit liability follows the network rules for EMV transactions. For networks with zero floor limits or for a merchant that approves a transaction above the network floor limits, the transaction may be cleared, but may not provide protection against insufficient funds.

Since a large number of cards, including those with the U.S. Common Debit AID, do not support EMV offline authorization, the merchant may want to perform deferred authorization as described in the next section.

Deferred Authorization

Definition: A deferred authorization is an authorization request or financial request (each hereafter referred to as "authorization") which occurs when a merchant captures transaction information while connectivity is interrupted; the merchant holds the transaction until connectivity is restored. After connectivity is restored, the merchant sends the transaction for an online authorization request, and receives an authorization response from the issuer.

Authorization: Deferred authorization occurs when an online authorization request is submitted to the issuer for authorization after the card has left the terminal. This can occur for an EMV transaction when the terminal requests an Authorization Request Cryptogram (ARQC) at the first Gen AC and the initial attempt to authorize the transaction cannot be completed due to a communication issue. The terminal does not receive a response to the online authorization request from the issuer, and the terminal and card resolve in an offline decline. Later, the merchant sends the authorization request to the issuer seeking a decision (approval or

[3] Generally, the U.S. Common Debit AIDs are online-only. However, if the appropriate infrastructure is built, there are no technical restrictions that would limit an issuer or network from using the offline features and capabilities of the chip. If the infrastructure were built across the industry and merchants desire to enable this acceptance, they should work with their acquirers regarding requirements. Network considerations include whether it plans to support the processing related to offline functionality. Issuer considerations include how the issuer chooses to personalize the card. In particular, the issuer would have to configure the card to support offline card authentication; and if they wish to support cardholder verification using PIN, they will have to enable and load the offline PIN. How an issuer decides to configure and personalize their cards can vary by issuer, product and even card.

decline). When submitting the authorization request, the merchant must include all standard EMV data (i.e., Field 55 data/DE 55, ARQC) as required in the deferred authorization request.[4]

Dual Message Clearing: Clearing requirements for approved deferred authorization transactions follow the same transaction flow as for online authorized transactions (i.e., authorization code, chip data as requested per network specifications). Deferred authorization declines from an issuer should not be processed for clearing (or re-submitted after issuer response). American Express and MasterCard require the Application Cryptogram to be submitted within the clearing record; the ARQC should be used for transactions that have been approved by the issuer. ***Please note:*** U.S. debit payment networks do not support batch clearing.

Pre-Authorization Completion: If the pre-authorization request was approved, then the network rules for completing the transaction apply, which may include the chip data (i.e., authorization code, chip data as requested per network specifications). If a pre-authorization request was declined or cannot process online, the completion should not be processed or re-submitted after issuer response.

- Single-Message (Debit): U.S. debit payment networks have varying methods as to how they allow the processing for deferred authorization transactions.[5] Merchants are only allowed one deferred online authorization decision. Any further attempts must be processed via the network exception processing system. For PULSE, SHAZAM and STAR, exception processing is not permitted. For single-message deferred authorization transactions, the financial transaction will settle the business day the transaction was re-submitted and approved online.

Liability: Deferred authorization transactions with chip data that receive an approved response follow same liability rules as chip transactions, based on network rules. In this case, while the merchant is waiting, they would typically make a risk decision to proceed with the transaction; but ultimately the merchant may be responsible for any loss incurred if the authorization is declined by the issuer and the customer is allowed to leave with the merchandise.

Force Post

Definition: Force post is where a merchant approves a transaction and processes the transaction into settlement without obtaining any issuer authorization.

Dual-Message Clearing (for Credit and Dual-Message Debit Transactions): Merchants must follow network requirements for clearing, including any EMV data, if required. Issuers should attempt to process a force post transaction unless the account is delinquent or has been closed/suspended due to fraud. ***Please note:*** U.S. debit payment networks do not support batch clearing.

Single Message (Debit): Merchants are encouraged to work with their acquirers/networks to determine support of a force post message. These transactions follow each network's specifications and rules and may include chip data.

Single-Message Adjustments (Debit): EMV data elements are not required for single message adjustments. Rather, adjustments for transactions not submitted in real-time must be keyed to the appropriate network's exception processing system in accordance with the applicable network's current process for single-message transaction adjustments.

Liability: The merchant may be ultimately responsible for losses incurred for any force post transaction when a chargeback is initiated. The dispute process follows the chargeback rules of the applicable network.

[4] If considering deferred authorization of PIN-based transactions, refer to PCI requirements around PIN.

[5] Networks included in the above statement include: Accel, AFFN, CU24, NYCE, PULSE, SHAZAM, and STAR.

Risk Management

For deferred authorization, force post or offline approvals above the applicable network floor limit, in order to mitigate risk, the merchant should consider the transaction amount and basket contents, and could evaluate the terminal verification result (TVR), if supported by the payment application on both the card and the terminal. This could, for example, help the merchant mitigate risk of accepting expired cards, cardholder verification method (CVM) failures, or counterfeit cards.

Note: Existing payment network chargeback rules apply.

Application Transaction Counter (ATC) Tracking: A card's ATC will invariably get out of sequence when transactions are performed offline or when deferred authorizations take place, especially if a cardholder makes multiple purchases at multiple locations within a short period of time. Payment networks caution issuers about declining transactions based on the ATC being out of sequence as it could result in unnecessary declines. A best practice is for issuers to use ATC for risk management related to duplicate transactions and reconciliation.

Legal Notice

While great effort has been made to ensure that the information in this document is accurate and current, this information does not constitute legal advice and should not be relied on for any legal purpose, whether statutory, regulatory, contractual or otherwise. All warranties of any kind are disclaimed, including all warranties relating to or arising in connection with the use of or reliance on the information set forth herein. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk.

Without limiting the foregoing, it is important to note that the information provided in this document is limited to the scenarios and payment networks specifically identified above, and that applicable rules, processing, liability and/or results may be impacted by specific facts or circumstances.

Additionally, each payment network determines its own policies and practices for processing transactions during communication disruptions (including but not limited to associated impact on liability), and all such policies and practices are subject to change.

Merchants, issuers, acquirers, processors and others implementing EMV chip technology in the U.S. are therefore strongly encouraged to consult with their respective payment networks regarding all applicable rules, requirements and procedures.

About the EMV Migration Forum

The EMV Migration Forum is a cross-industry body focused on supporting the EMV chip implementation steps required for payment networks, issuers, processors, merchants, and consumers to help ensure a successful introduction of more secure chip technology in the United States. The focus of the Forum is to address topics that require some level of industry cooperation and/or coordination to migrate successfully to chip technology in the United States. For more information on the EMV Migration Forum, please visit http://www.emv-connection.com/emv-migration-forum/

Copyright Notice