TRANSACTION RESPONSE AND RESULT CODES

This document provides information concerning the codes that are returned in LitleXML responses for payment transactions. For information about LitleXML response codes for chargeback transactions, see the *Chargeback API Reference Guide*. This document contains the following sections:

PAYMENT TRANSACTION RESPONSE CODES

This section contains a list of codes and messages that the system can return in the LitleXML response for a payment transaction.

NOTE: **For information concerning Chargeback Response Code, see the *Chargeback API Reference Guide*.**

Table 1 shows all possible values for the `<response>` and `<message>` elements along with a recommended action, if applicable. Hard declines are shown in **bold** type.

- The Response Code value appears in the `<response>` element.
- The Response Message value appears in the `<message>` element.

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
000	Approved	Approved	No action required.
010	Partially Approved	Approved	The authorized amount is less than the requested amount.
011	Offline Approval	Approved	Offline approval issued while the terminal is unable to communicate with the issuer.
013	Offline Approval (unable to go online)	Approved	Offline approval issued while the terminal is unable to communicate with the issuer.
100	Processing Network Unavailable	Soft Decline	There is a problem with the card network. Contact the network for more information.
101	Issuer Unavailable	Soft Decline	There is a problem with the issuer network. Please contact the issuing bank.
102	Re-submit Transaction	Soft Decline	There is a temporary problem with your submission. Please re-submit the transaction.
110	Insufficient Funds	Soft Decline	The card does not have enough funds to cover the transaction.
111	**Authorization amount has already been depleted**	**Hard Decline**	**The total amount of the original Authorization has been used.**
120	Call Issuer	Referral or Soft Decline	There is an unspecified problem, contact the issuing bank.
121	Call AMEX	Referral	There is an unspecified problem; contact AMEX.
122	Call Diners Club	Referral	There is an unspecified problem; contact Diners Club.
123	Call Discover	Referral	There is an unspecified problem; contact Discover.
124	Call JBS	Referral	There is an unspecified problem; contact JBS.
125	Call Visa/MasterCard	Referral	There is an unspecified problem; contact Visa or MasterCard.
126	Call Issuer - Update Cardholder Data	Referral	Some data is out of date; contact the issuer to update this information.
127	**Exceeds Approval Amount Limit**	**Hard Decline**	**This transaction exceeds the daily approval limit for the card or the PayPal user account.**

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
130	Call Indicated Number	Referral	There is an unspecified problem; contact the phone number provided.
140	Update Cardholder Data	Referral	Cardholder data is incorrect; contact the issuing bank.
191	The merchant is not registered in the update program.	N/A	This is an Account Updater response indicating a set-up problem that must be resolved prior to submitting another request file. Escalate this to your Customer Experience Manager.
192	**Merchant is not certified/enabled for IIAS**	**Hard Decline**	**Your organization is not certified or enabled for IIAS/FSA transactions.**
206	Issuer Generated Error	Soft Decline	An un spec ife id error was returned by the issuer. Please retry the transaction and if the problem persists, contact the issuing bank.
207	**Pickup card - Other than Lost/Stolen**	**Hard Decline**	**The issuer indicated that the gift card should be removed from use.**
209	**Invalid Amount**	**Hard Decline**	**The specified amount is invalid for this transaction.**
211	**Reversal Unsuccessful**	**Hard Decline**	**The reversal transaction was unsuccessful.**
212	**Missing Data**	**Hard Decline**	**Contact Vantiv.**
213	**Pickup Card - Lost Card**	**Hard Decline**	**The submitted card was reported as lost and should be removed from use.**
214	**Pickup Card - Stolen Card**	**Hard Decline**	**The submitted card was reported as stolen and should be removed from use.**
215	**Restricted Card**	**Hard Decline**	**The specified Gift Card is not available for use.**
216	**Invalid Deactivate**	**Hard Decline**	**The Deactivate transaction is invalid for the specified card.**
217	**Card Already Active**	**Hard Decline**	**The submitted card is already active.**
218	**Card Not Active**	**Hard Decline**	**The submitted card has not been activated.**

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
219	Card Already Deactivate	Hard Decline	The submitted card has already been deactivated.
221	Over Max Balance	Hard Decline	The activate or load amount exceeds the maximum allowed for the specified gift Card.
222	Invalid Activate	Hard Decline	The activate transaction is not valid or can no longer be reversed.
223	No transaction Found for Reversal	Hard Decline	The transaction referenced in the reversal transaction does not exist.
226	Incorrect CVV	Hard Decline	The transaction was declined because it was submitted with the incorrect security code.
229	Illegal Transaction	Hard Decline	The transaction would violate the law.
251	Duplicate Transaction	Hard Decline	The transaction is a duplicate of a previously submitted transaction.
252	System Error	Hard Decline	Contact Vantiv.
253	Deconverted BIN	Hard Decline	The BIN is no longer valid.
254	Merchant Depleted	Hard Decline	No balance remains on gift Card.
255	Gift Card Escheated	Hard Decline	The Gift Card has been seized by the government while resolving an estate.
256	Invalid Reversal Type for Credit Card Transaction	Hard Decline	You attempted to use a Closed Loop Gift Card reversal transaction to reverse a credit card transaction. For example, you cannot use a a Deposit Reversal transaction to reverse a Capture. To reverse a credit card Capture transaction, use a Credit transaction.
257	System Error (message format error)	Hard Decline	The issuer has reported that the message format is incorrect. Contact Vantiv.
258	System Error (cannot process)	Hard Decline	The issuer has reported that the transaction could not be processed. Contact Vantiv.

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
301	Invalid Account Number	Hard Decline	The account number is not valid; contact the cardholder to confirm information or inquire about another form of payment.
302	Account Number Does Not Match Payment Type	Hard Decline	The payment type was selected as one card type (e.g. Visa), but the card number indicates a different card type (e.g. MasterCard).
303	Pick Up Card	Hard Decline	This is a card present response, but in a card not present environment. Do not process the transaction and contact the issuing bank.
304	Lost/Stolen Card	Hard Decline	The card has been designated as lost or stolen; contact the issuing bank.
305	Expired Card	Hard Decline	The card is expired.
306	Authorization has expired; no need to reverse	Hard Decline	The original Authorization is no longer valid, because it has expired. You can not perform an Authorization Reversal for an expired Authorization.
307	Restricted Card	Hard Decline	The card has a restriction preventing approval for this transaction. Please contact the issuing bank for a specific reason. You may also receive this code if the transaction was declined due to Prior Fraud Advice Filtering and you are using a schema version V8.10 or older.
308	Restricted Card - Chargeback	Hard Decline	The card has a restriction preventing approval if there are any chargebacks against it.
309	Restricted Card - Prepaid Card Filtering Service	Hard Decline	This transaction is being declined due the operation of the Prepaid Card Filtering service.
310	Invalid track data	Hard Decline	The track data is not valid.
311	Deposit is already referenced by a chargeback	Hard Decline	The deposit is already referenced by a chargeback; therefore, a refund cannot be processed against the original transaction.
312	Restricted Card - International Card Filtering Service	Hard Decline	This transaction is being declined due the operation of the International Card Filtering service.

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
313	**International filtering for issuing card country <country>** (where <country> is the 3-character country code)	**Hard Decline**	**This is returned when the transaction involves a US based merchant processing Canadian transactions has a transaction that uses a US card.**
315	**Restricted Card - Auth Fraud Velocity Filtering Service**	**Hard Decline**	**This transaction is being declined due the operation of the Auth Fraud Velocity Filtering Service.**
316	**Automatic Refund Already Issued**	**Hard Decline**	**This refund transaction is a duplicate for one already processed automatically by the Fraud Chargeback Prevention Service (FCPS).**
318	**Restricted Card - Auth Fraud Advice Filtering Service**	**Hard Decline**	**This transaction is being declined due the operation of the Auth Fraud Advice Filtering Service.**
319	**Restricted Card - Fraud AVS Filtering Service**	**Hard Decline**	**This transaction is being declined due the operation of the Auth Fraud AVS Filtering Service.**
320	**Invalid Expiration Date**	**Hard Decline**	**The expiration date is invalid.**
321	**Invalid Merchant**	**Hard Decline**	**The card is not allowed to make purchases from this merchant (e.g. a Travel only card trying to purchase electronics).**
322	**Invalid Transaction** **Note:** If you are enabled for Transaction Filtering, but have not upgraded to use schema version 8.3 or above, the system returns this code for transactions filtered by the Prepaid or International Card Filtering Service. Also, if you are enabled for Velocity Fraud Filtering, but have not upgraded to V8.9, you will receive this code for filtered transactions.	**Hard Decline**	**The transaction is not permitted; contact the issuing bank.**

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
323	No such issuer	Hard Decline	The card number references an issuer that does not exist. Do not process the transaction.
324	Invalid Pin	Hard Decline	The PIN provided is invalid.
325	Transaction not allowed at terminal	Hard Decline	The transaction is not permitted; contact the issuing bank.
326	Exceeds number of PIN entries	Hard Decline	(Referring to a debit card) The incorrect PIN has been entered excessively and the card is locked.
327	Cardholder transaction not permitted	Hard Decline	The card is restricted for purchases. (For example, travel and entertainment only.)
328	Cardholder requested that recurring or installment payment be stopped	Hard Decline	Recurring/Installment Payments no longer accepted by the card issuing bank, or the PayPal account holder cancelled the recurring/installment billing agreement on their account.
330	Invalid Payment Type	Hard Decline	This payment type is not accepted by the issuer.
331	Invalid POS Capability for Cardholder Authorized Terminal Transaction	Hard Decline	For a Cardholder Authorized Terminal Transaction the POS capability must be set to magstripe.
332	Invalid POS Cardholder ID for Cardholder Authorized Terminal Transaction	Hard Decline	For a Cardholder Authorized Terminal Transaction the POS Cardholder ID must be set to nopin.
335	This method of payment does not support authorization reversals.	Hard Decline	You can not perform an Authorization Reversal transaction for this payment type.
336	Reversal amount does not match Authorization amount.	Hard Decline	For a merchant initiated reversal against an American Express authorization, the reversal amount must match the authorization amount exactly.
340	Invalid Amount	Hard Decline	The transaction amount is invalid (too high or too low). For example, less than 0 for an authorization, or less than .01 for other payment types.

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
341	**Invalid Healthcare amounts**	**Hard Decline**	**The amount submitted with this FSA/Healthcare transaction is invalid. The FSA amount must be greater than 0, and cannot be greater than the transaction amount.**
346	**Invalid billing descriptor prefix**	**Hard Decline**	**The billing descriptor prefix submitted is not valid.**
347	**Invalid billing descriptor**	**Hard Decline**	**The billing descriptor is not valid because you are not authorized to send transactions with custom billing fields.**
348	**Invalid Report Group**	**Hard Decline**	**The Report Group specified in the transaction is invalid, because it is either not in the defined list of acceptable Report Groups or there is a mis-match between the Report Group and the defined Billing Descriptor.**
349	Do Not Honor	Soft Decline	The issuing bank has put a temporary hold on the card.
350	Generic Decline	Soft or **Hard Decline**	There is an unspecified problem; contact the issuing bank for more details. **Note**: This code can be a hard or soft decline, depending on the method of payment, and other variables.
351	Decline - Request Positive ID	Hard Decline	Card Present transaction that requires a picture ID match.
352	**Decline CVV2/CID Fail**	**Hard Decline**	**The CVV2/CID is invalid.**
354	**3-D Secure transaction not supported by merchant**	**Hard Decline**	**You are not certified to submit 3-D Secure transactions.**
356	Invalid purchase level III, the transaction contained bad or missing data	Soft Decline	Submitted Level III data is bad or missing.
357	**Missing healthcare IIAS tag for FSA transaction**	**Hard Decline**	**The FSA Transactions submitted does not contain the <`healtcareIIAS`> data element.**
358	**Restricted by Litle due to security code mismatch.**	**Hard Decline**	**The transaction was declined due to the security code (CVV2, CID, etc) not matching.**

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
360	**No transaction found with specified litleTxnId**	**Hard Decline**	**There were no transactions found with the specified litleTxnId.**
361	**Authorization no longer available**	**Hard Decline**	**The authorization for this transaction is no longer available. Either the authorization has already been consumed by another capture, or the authorization has expired.**
362	**Transaction Not Voided - Already Settled**	**Hard Decline**	**This transaction cannot be voided; it has already been delivered.**
363	**Auto-void on refund**	**Hard Decline**	**This transaction (both capture and refund) has been voided.**
364	**Invalid Account Number - original or NOC updated eCheck account required**	**Hard Decline**	**The submitted account number is invalid. Confirm the original account number or check NOC for new account number.**
365	**Total credit amount exceeds capture amount**	**Hard Decline**	**The amount of the credit is greater than the capture, or the amount of this credit plus other credits already referencing this capture are greater than the capture amount.**
366	**Exceed the threshold for sending redeposits**	**Hard Decline**	**NACHA rules allow two redeposit attempts within 180 days of the settlement date of the initial deposit attempt. This threshold has been exceeded.**
367	**Deposit has not been returned for insufficient/non-sufficient funds**	**Hard Decline**	**NACHA rules only allow redeposit attempts against deposits returned for Insufficient or Uncollected Funds.**
368	Invalid check number	Soft Decline	The check number is invalid.
369	**Redeposit against invalid transaction type**	**Hard Decline**	**The redeposit attempted against an invalid transaction type.**
370	**Internal System Error - Call Litle**	**Hard Decline**	**There is a problem with the System. Contact support@litle.com.**
372	Soft Decline - Auto Recycling in Progress	Soft Decline	The transaction was intercepted because it is being auto recycled by the Recycling Engine.
373	**Auto Recycling Complete**	**Hard Decline**	**The transaction was intercepted because auto recycling has completed with a final decline.**

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
375	Merchant is not enabled for surcharging	Hard Decline	The submitted transaction contained a surcharge and the merchant is not enabled for surcharging.
376	This method of payment does not support surcharging	Hard Decline	The use of a surcharge is only allowed for Visa and MasterCard methods of payment.
377	Surcharge is not valid for debit or prepaid cards	Hard Decline	You cannot apply a surcharge to a transaction using a debit or prepaid card.
378	Surcharge cannot exceed 4% of the sale amount	Hard Decline	The surcharge in the submitted transaction exceeded 4% maximum allowed for a surcharge.
380	Secondary amount cannot exceed the sale amount	Hard Decline	The secondary amount exceeded the sale amount in the submitted transaction.
381	This method of payment does not support secondary amount	Hard Decline	The submitted method of payment does not allow the use of Convienence Fees.
382	Secondary amount cannot be less than zero	Hard Decline	The secondary amount must be a positive integer.
383	Partial transaction is not supported when including a secondary amount	Hard Decline	Transactions set to allow partial authorizations cannot include a secondary amount.
384	Secondary amount required on partial refund when used on deposit	Hard Decline	If the associated sale or capture transaction included a secondary amount, an associated partial refund must include a secondary amount.
385	Secondary amount not allowed on refund if not included on deposit	Hard Decline	If the associated sale or capture transaction did not included a secondary amount, you cannot include a secondary amount on an assciated refund.
401	Invalid E-mail	Hard Decline	The e-mail address provided is not valid. Verify that it was entered correctly.

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
469	**Invalid Recurring Request - See Recurring Response for Details**	**Hard Decline**	**The Recurring Request was invalid, which invalidated the transaction. The Response Code and Message in the Recurring Response contains additional information.**
470	Approved - Recurring Payment Scheduled	Approved	The recurring request was processed successfully.
471	**Parent Transaction Declined - Recurring Subscription Not Created**	**Hard Decline**	**The parent payment transaction was declined, so the recurring payments have not been scheduled.**
472	**Invalid Billing Plan**	**Hard Decline**	**The plan specified in the recurring request was invalid.**
473	Scheduled Recurring Payment Processed	Approved	The scheduled recurring payment has been processed successfully.
475	**Invalid Subscription Id**	**Hard Decline**	**The referenced subscription Id does not exist.**
476	**Add On Code Already Exists**	**Hard Decline**	**The specified Adoo On code already exists.**
477	**Duplicate Add On Codes in Requests**	**Hard Decline**	**Multiple createAddOn requests submitted with the same Add On Code.**
478	**No Matching Add On Code for the Subscription**	**Hard Decline**	**The Add On code specified does not exist.**
480	**No Matching Discount Code for the Subscription**	**Hard Decline**	**The Discount Code supplied in the updateDiscount or deleteDiscount transaction does not exist.**
481	**Duplicate Discount Codes in Request**	**Hard Decline**	**Multiple createDiscount requests submitted with the same Discount Code.**
482	**Invalid Start Date**	**Hard Decline**	**The supplied Start Date is invalid.**
483	**Merchant Not Registered for Recurring Engine**	**Hard Decline**	**You are not registered for the use of the Recurring Engine.**
500	**The account number was changed**	**Hard Decline**	**An Account Updater response indicating the Account Number changed from the original number.**

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
501	**The account was closed**	**Hard Decline**	**An Account Updater response indicating the account was closed. Contact the cardholder directly for updated information.**
502	The expiration date was changed	N/A	An Account Updater response indicating the Expiration date for the card has changed.
503	The issuing bank does not participate in the update program	N/A	An Account Updater response indicating the issuing bank does not participate in the update program
504	Contact the cardholder for updated information	N/A	An Account Updater response indicating you should contact the cardholder directly for updated information.
505	No match found	N/A	An Account Updater response indicating no match was found in the updated information.
506	No changes found	N/A	An Account Updater response indicating there have been no changes to the account information.
530	**Apple Pay Key Mismatch**	**Hard**	**The submitted publicKeyHash element does not match any configured entries. Contact your Implementation Consultant.**
531	**Apple Pay Decryption Failed**	**Hard**	**Vantiv was unable to decrypt the submitted information.**
550	**Restricted Device or IP - ThreatMetrix Fraud Score Below Threshold**	**Hard Decline**	**The transaction was declined because the resulting ThreatMetrix Fraud Sorce was below the acceptable threshold set in the merchant's policty.**
601	Soft Decline - Primary Funding Source Failed	Soft Decline	A PayPal response indicating the transaction failed due to an issue with primary funding source (e.g. expired Card, insufficient funds, etc.).
NOTE:	**The Response Message associated with Response Code 602 is inaccurate due to a remapping of PayPal Response Codes. Please read the Description below for the recommended action when receiving Response Code 602.**		

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
602	Soft Decline - Buyer has alternate funding source	Soft Decline	The transaction could not be completed for one of the following reasons: • The billing address associated with the financial Instrument could not be confirmed. • The transaction exceeds the card limit. • The transaction was denied by the card issuer. You should establish error handling logic that directs the customer to contact PayPal to resolve the issue with their account.
610	**Hard Decline - Invalid Billing Agreement Id**	**Hard Decline**	**A PayPal response indicating the Billing Agreement ID is invalid.**
611	**Hard Decline - Primary Funding Source Failed**	**Hard Decline**	**A PayPal response indicating the issuer is unavailable.**
612	**Hard Decline - Issue with Paypal Account**	**Hard Decline**	**A PayPal response indicating the transaction failed due to an issue with the buyer account.**
613	**Hard Decline - PayPal authorization ID missing**	**Hard Decline**	**A PayPal response indicating the need to correct the authorization ID before resubmitting.**
614	**Hard Decline - confirmed email address is not available**	**Hard Decline**	**A PayPal response indicating your account is configured to decline transactions without a confirmed address. request another payment method or contact support@litle.com to modify your account settings.**
615	**Hard Decline - PayPal buyer account denied**	**Hard Decline**	**A PayPal response indicating account unauthorized payment risk.**
616	**Hard Decline - PayPal buyer account restricted**	**Hard Decline**	**A PayPal response indicating PayPal is unable to process the payment. Buyer should contact PayPal with questions.**
617	**Hard Decline - PayPal order has been voided, expired, or completed**	**Hard Decline**	**A PayPal response indicating no further authorizations/captures can be processed against this order. A new order must be created.**

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
618	Hard Decline - issue with PayPal refund	Hard Decline	A PayPal response indicating one of these potential refund-related issues: duplicate, partial refund must be less than or equal to original or remaining amount, past time limit, not allowed for transaction type, consumer account locked/inactive, or complaint exists - only a full refund of total/remaining amount allowed. Contact support@litle.com for specific details.
619	Hard Decline - PayPal credentials issue	Hard Decline	A PayPal response indicating you do not have permissions to make this API call.
620	Hard Decline - PayPal authorization voided or expired	Hard Decline	A PayPal response indicating you cannot capture against this authorization. You need to perform a brand new authorization for the transaction.
621	Hard Decline - required PayPal parameter missing	Hard Decline	A PayPal response indicating missing parameters are required. Contact support@litle.com for specific details.
622	Hard Decline - PayPal transaction ID or auth ID is invalid	Hard Decline	A PayPal response indicating the need to check the validity of the authorization ID prior to reattempting the transaction.
623	Hard Decline - Exceeded maximum number of PayPal authorization attempts	Hard Decline	A PayPal response indicating you should capture against a previous authorization.
624	Hard Decline - Transaction amount exceeds merchant's PayPal account limit.	Hard Decline	A PayPal response indicating the transaction amount exceeds the merchant's account limit. Contact support@litle.com to modify your account settings.
625	Hard Decline - PayPal funding sources unavailable.	Hard Decline	A PayPal response indicating the buyer needs to add another funding sources to their account.
626	Hard Decline - issue with PayPal primary funding source.	Hard Decline	A PayPal response indicating there are issues with the buyer's primary funding source.

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
627	**Hard Decline - PayPal profile does not allow this transaction type.**	**Hard Decline**	**Contact us to adjust your PayPal merchant profile preferences.**
628	**Internal System Error with PayPal - Contact Litle**	**Hard Decline**	**There is a problem with the username and password. Contact support@litle.com.**
629	**Hard Decline - Contact PayPal consumer for another payment method.**	**Hard Decline**	**A PayPal response indicating that you must contact the consumer for another payment method.**
637	**Invalid terminal Id**	**Hard Decline**	**The terminal Id submitted with the POS transaction is invalid.**
701	**Under 18 years old**	**Hard Decline**	**A Bill Me Later (BML) response indicating the customer is under 18 years of age based upon the date of birth.**
702	**Bill to outside USA**	**Hard Decline**	**A BML response indicating the billing address is outside the United States.**
703	**Bill to address is not equal to ship to address**	**Hard Decline**	**A BML response indicating that the billing address does not match the shipping address.**
704	**Declined, foreign currency, must be USD**	**Hard Decline**	**A BML response indicating the transaction is declined, because it is not in US dollars.**
705	**On negative file**	**Hard Decline**	**A BML response indicating the account is on the negative file.**
706	**Blocked agreement**	**Hard Decline**	**A BML response indicating a blocked agreement account status.**
707	Insufficient buying power	Other	A BML response indicating that the account holder does not have sufficient credit available for the transaction amount.
708	**Invalid Data**	**Hard Decline**	**A BML response indicating that there are one or more problems with the submitted data.**
709	**Invalid Data - data elements missing**	**Hard Decline**	**A BML response indicating one or more required data elements are missing.**
710	**Invalid Data - data format error**	**Hard Decline**	**A BML response indicating that some data was formatted incorrectly.**

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
711	**Invalid Data - Invalid T&C version**	**Hard Decline**	**A BML response indicating the T&C version is invalid.**
712	**Duplicate transaction**	**Hard Decline-**	**A BML response indicating that the transaction is a duplicate.**
713	**Verify billing address**	**Hard Decline**	**A BML response indicating that you should verify the billing address.**
714	**Inactive Account**	**Hard Decline**	**A BML response indicating the customer account is inactive.**
716	**Invalid Auth**	**Hard Decline**	**A BML response indicating that the referenced authorization is invalid.**
717	**Authorization already exists for the order**	**Hard Decline**	**A BML response indicating that an authorization already exists for the transaction.**
801	Account number was successfully registered	Approved	The card number was successfully registered and a token number was returned.
802	Account number was previously registered.	Approved	The card number was previously registered for tokenization.
805	Card Validation Number Updated	Approved	The stored value for CVV2/CVC2/CID has been successfully updated.
820	**Credit card number was invalid**	**Hard Decline**	**The card number submitted for tokenization is invalid.**
821	**Merchant is not authorized for tokens**	**Hard Decline**	**Your organization is not authorized to use tokens.**
822	**Token was not found**	**Hard Decline**	**The token number submitted with this transaction was not found.**
850	**Tax Billing only allowed for MCC 9311**	**Hard Decline**	**Tax Billing elements are allowed only for MCC 9311.**
851	**Incomplete Tax Billing**	**Hard Decline**	**Missing taxType element**
852	**Debt Repayment only allowed for VI transactions on MCCs 6012 and 6051**	**Hard Decline**	**You must be either MCC 6012 or 6051 to designate a Visa transaction as Debt Repayment (debtRepayment element set to true).**
877	**Invalid Pay Page Registration Id**	**Hard Decline**	**A Pay Page response indicating that the Pay Page Registration ID submitted is invalid.**

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
878	**Expired Pay Page Registration Id**	**Hard Decline**	**A Pay Page response indicating that the Pay Page Registration ID has expired (Pay Page Registration IDs expire 24 hours after being issued).**
879	**Merchant is not authorized for Pay Page**	**Hard Decline**	**Your organization is not authorized to use the Pay Page.**
898	Generic token registration error	Soft Decline	There is an unspecified token registration error; contact your Customer Experience Manager.
899	Generic token use error	Soft Decline	There is an unspecified token use error; contact your Customer Experience Manager.
900	**Invalid Bank Routing Number**	**Hard Decline**	**The eCheck routing number submitted with this transaction has failed validation.**
901	**Missing Name**	**Hard Decline**	**The customer name is required for SEPA transactions.**
902	**Invalid Name**	**Hard Decline**	**The customer name must be a minimum of two characters for SEPA transactions.**
903	**Missing Billing Country Code**	**Hard Decline**	**The Billing Country code is required for SEPA transactions.**
904	**Invalid IBAN**	**Hard Decline**	The submitted International Bank Account number is invalid. Please correct the number and resubmit the traction.
905	**Missing Email Address**	**Hard Decline**	**The customer email addres is required for SEPA transactions.**
950	**Decline - Negative Information on File**	**Hard Decline**	**An eCheck response indicating the account is on the negative file.**
951	**Absolute Decline**	**Hard Decline**	**An eCheck response indicating that this transaction was declined.**
952	**The Merchant Profile does not allow the requested operation.**	**Hard Decline**	**An eCheck response indicating that your Merchant Profile does not allow the requested operation. Contact your Customer Experience Manager for additional information.**
953	**The account cannot accept ACH transactions.**	**Hard Decline**	**An eCheck response indicating the customer's checking account does not accept ACH transactions.**

TABLE 1 Transaction Response Codes

Response Code	Response Message	Response Type	Description
954	The account cannot accept ACH transactions or site drafts.	Hard Decline	An eCheck response indicating the customer's checking account does not accept ACH transactions or site drafts.
955	Amount greater than limit specified in the Merchant Profile.	Hard Decline	An eCheck response indicating that the dollar amount of this transaction exceeds the maximum amount specified in your Merchant Profile. Contact your Customer Experience Manager for additional information.
956	Merchant is not authorized to perform eCheck Verification transactions.	Hard Decline	An eCheck response indicating that your organization is not authorized to perform eCheck verifications. Contact your Customer Experience Manager for additional information.
957	First Name and Last Name required for eCheck Verifications.	Hard Decline	An eCheck response indicating that the first and last name of the customer is required for eCheck verifications.
958	Company Name required for corporate account for eCheck Verifications.	Hard Decline	An eCheck response indicating that the company name is required for verifications on corporate accounts.
959	Phone number required for eCheck Verifications	Hard Decline	An eCheck response indicating that the phone number of the customer is required for eCheck verifications.
961	Card Brand token not supported	Hard Decline	This code is returned if the merchant submits a Visa generated token.
962	Private Label Card not supported	Hard Decline	This code is returned if the transaction involves a Visa Private Label card.

3DSAUTHENTICATION RESULT CODES

Table 2 contains a list of valid authentication result codes returned by Visa for the Verified by Visa service or MasterCard for the MasterCard SecureCode service. It specifies what authentication result values apply to what order sources.

TABLE 2 3DS Authentication Response Codes

Authentication Result Code	Description
Order Source - Ecommerce	
Blank	Standard e-commerce or non-e-commerce transactions, not an authentication or attempted authentication. The CAVV is not present.
Order Source - any	
B	CAVV passed verification but no liability shift because a) ECI was not 5, 6, or b) the card type is an excluded (e.g. Commercial Card).
Order Source - 3DSAuthenticated or 3DSAttempted	
0	CAVV data field not properly formatted; verification cannot be performed.
6	CAVV not verified because Issuer has requested no verification. VisaNet processes as if CAVV is valid.
Order Source - 3DSAuthenticated	
1	CAVV failed verification.
2	CAVV passed verification.
D	Issuer elected to return CAVV verification results and Field 44.13 is blank. This value is set by VisaNet; it indicates that CAVV results are valid.
Order Source - 3DSAttempted	
3	CAVV passed verification.
4	CAVV failed verification.
5	For future use; value not currently used.
7	CAVV failed verification.
8	CAVV passed verification.
9	CAVV failed verification; Visa generated CAVV because the Issuer ACS was not available.
A	CAVV passed verification; Visa generated CAVV because this Issuer ACS was not available.

TABLE 2 3DS Authentication Response Codes

Authentication Result Code	Description
B	CAVV passed verification but no liability shift because a) ECI was not 5 or 6, or b) the card type is an excluded (e.g., Commercial Card)
C	Issuer elected to return CAVV verification results and Field 44.13 is blank. Value is set by VisaNet; indicates that CAVV Results are valid.

AVS Response Codes

Table 3 contains a list of AVS response codes that can be returned in the response for a payment transaction. Although there are some codes that a particular merchant may never receive, Vantiv recommends you code your system to expect all codes from this list.

NOTE: The response does not include the description shown in the table below.

TABLE 3 AVS Response Codes

AVS Response Code	Description
00	5-Digit zip and address match
01	9-Digit zip and address match
02	Postal code and address match
10	5-Digit zip matches, address does not match
11	9-Digit zip matches, address does not match
12	Zip does not match, address matches
13	Postal code does not match, address matches
14	Postal code matches, address not verified
20	Neither zip nor address match
30	AVS service not supported by issuer
31	AVS system not available

TABLE 3 AVS Response Codes

AVS Response Code	Description
32	Address unavailable
33	General error
34	AVS not performed
40	Address failed Litle & Co. edit checks

ADVANCED AVS RESPONSE CODES

Table 4 contains a list of American Express Advanced AVS response codes that can be returned as verification of information supplied in the <name>, <phone> and/or <email> child elements of the <billToAddress> element. The system returns the AAVS response code in the <advancedAVSResult> child of the <fraudResult> element.

NOTE: **You must be certified to use LitleXML version 7.3 or above and specifically enabled to use the Advanced AVS feature. Please consult your Customer Experience Manager for additional information.**

The code returned has the following format:

- **1st position** - name match
- **2nd position** - phone match
- **3rd position** - email match
- Each position can have one of the following values:
  - **0** - No Match (failure)
  - **1** - Match
  - **2** - Not Sent
  - **3** - No Response (unchecked, retry, or service not allowed)

For example, a code of 210 would indicate that the name was not sent, the phone matches, and the email does not match.

You should code your system to parse all codes from this list. The description is not included in the response.

TABLE 4 Advanced AVS Response Codes

AAVS Response Code	Description
000	No Match
001	Email matches, name and phone do not match
002	Name and phone do not match, email not sent
003	Name and phone do not match, no response for email
010	Phone matches, name and email do not match
011	Phone and email match, name does not match
012	Phone matches, name does not match, email not sent
013	Phone matches, name does not match, no response for email
020	Name and email do not match, phone not sent
021	Email matches, name does not match, phone not sent
030	Name and email do not match, no response for phone
031	Email matches, name does not match, no response for phone
033	Name does not match, no response for phone or email
100	Name matches, phone and email do not match
101	Name and email match, phone does not match
102	Name matches, phone does not match, email not sent
103	Name matches, phone does not match, no response for email
110	Name and phone match, no response for email
111	Full match
112	Name and phone match, email not sent
113	Name and phone match, no response for email
120	Name matches, email does not match, phone not sent
121	Name and email match, phone not sent

TABLE 4 Advanced AVS Response Codes

AAVS Response Code	Description
130	Name matches, email does not match, no response for phone
131	Name and email match, no response for phone
133	Name matches, no response for phone or email
200	Name not sent, phone and email do not match
201	Email matches, phone does not match, name not sent
202	Phone does not match, name and email not sent
203	Phone does not match, name not sent, no response for email
210	Phone matches, email does not match, name not sent
211	Phone and email match, name not sent
212	Phone matches, name and email not sent
213	Phone matches, name not sent, no response for email
220	Email does not match, name and phone not sent
221	Email matches, name and phone not sent
230	Email does not match, name not sent, no response for phone
231	Email matches, name not sent, no response for phone
233	Name not sent, no response for phone and email
300	Phone and email do not match, no response for name
301	Email matches, phone does not match, no response for name
302	Phone does not match, no response for name, email not sent
303	Phone does not match, no response for name and email
310	Phone matches, email does not match, no response for name
311	Phone and email match, no response for name
312	Phone matches, email not sent, no response for name

TABLE 4 Advanced AVS Response Codes

AAVS Response Code	Description
313	Phone matches, no response for name and email
320	Email does not match, phone not sent, no response for name
321	Email matches, phone not sent, no response for name
330	Email does not match, no response for name and phone
331	Email matches, no response for name and phone
333	No response

CARD VALIDATION RESPONSE CODES

Table 5 contains a list of possible response codes returned when requesting a card validation check.

- CVV2
- CVC2
- CID

The description is not included in the response to the merchant.

NOTE: **You must be registered with American Express for this service. Also, AMEX does not return card validation response codes. Instead, if the check fails, you receive Response Reason Code 352 for the transaction.**

TABLE 5 Card Validation Response Codes

CVV2/CVC2/CID Response Code	Description
M	Match
N	No Match
P	Not Processed
S	CVV2/CVC2/CID should be on the card but the merchant has indicated CVV2/CVC2/CID is not present.

TABLE 5 Card Validation Response Codes

CVV2/CVC2/CID Response Code	Description
U	Issuer is not certified for CVV2/CVC2/CID processing.
"" (empty response)	A check was not done for an unspecified reason.

ADVANCED FRAUD TOOLS TRIGGERED RULES

This section provides definitions of the triggered rules returned in the Advanced Fraud Results (`advancedFraudResults` element) section of the response message (see Example below). ThreatMetrix uses the rules triggered by each advanced fraud check to determine the device reputation score, which in turn determines the final review status: Pass, Review, or Fail.

NOTE: **The rules/descriptions in this document reflect those used in the generic merchant policy. Depending upon the policy configured in your merchant profile, some rules may not apply to you, or additional rules, not defined here, may appear in your results.**

Example: advancedFraudResults Structure

```
<advancedFraudResults>
  <deviceReviewStatus>pass, fail, review, etc.</deviceReviewStatus>
  <deviceReputationScore>Score Returned from ThreatMetrix</deviceReputationScore>
  <triggeredRule>Triggered Rule #1</triggeredRule>
  .
  .
  .
  <triggeredRule>Triggered Rule #N</triggeredRule>
</advancedFraudResults>
```

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
10PaymentsOnDeviceLocalDay	This device has submitted 10 or more payments in the previous 24 hours. This is atypical and may be an indicator of misuse.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
10PaymentsOnDeviceLocalHour	This device has submitted 10 or more payments in the previous hour. This is atypical and may be an indicator of misuse.
10PaymentsOnFuzzyDeviceLocalDay	This device appears to have submitted 10 or more payments in the previous 24 hours. This is atypical and may be an indicator of misuse.
10PaymentsOnFuzzyDeviceLocalHour	This device appears to have submitted 10 or more payments in the previous hour. This is atypical and may be an indicator of misuse.
10PaymentsOnTrueIPLocalDay	This True IP has submitted 10 or more payments in the previous day. This is atypical and may be an indicator of misuse.
10PaymentsOnTrueIPLocalHour	This True IP submitted 10 or more payments in the previous hour. This is atypical and may be an indicator of misuse.
10PaymentsWithEmailAddressLocalDay	This email address has submitted 10 or more payments in the previous day. This is atypical and may be an indicator of misuse.
15PaymentsWithCustomerIDLocalDay	This customer ID submitted 15 or more payments in the previous day. This is atypical and may be an indicator of misuse.
15PaymentsWithPaymentCardLocalDay	This payment card submitted 15 or more payments in the previous day. This is atypical and may be an indicator of misuse.
100PaymentsOnDeviceLocalMonth	This device has submitted 100 or more payments in the previous month. This is atypical and may be an indicator of misuse.
100PaymentsOnFuzzyDeviceLocalMonth	This device appears to have submitted 100 or more payments in the previous month. This is atypical and may be an indicator of misuse.
100PaymentsOnTrueIPLocalMonth	This True IP has submitted 100 or more payments in the previous month. This is atypical and may be an indicator of misuse.
2ScreenResolutionsPerDeviceGlobalDay	This device has used 2 or more screen resolutions in the past day. This is atypical and may indicate misuse.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
20PaymentsOnDeviceLocalDay	This device has submitted 20 or more payments in the previous 24 hours. This is atypical and may be an indicator of misuse.
20PaymentsOnFuzzyDeviceLocalDay	This device appears to have submitted 20 or more payments in the previous 24 hours. This is atypical and may be an indicator of misuse.
20PaymentsOnTrueIPLocalDay	This True IP has submitted 20 or more payments in the previous day. This is atypical and may be an indicator of misuse.
20PaymentsWithCustomerIDLocalWeek	This customer ID submitted 20 or more payments in the previous week. This is atypical and may be an indicator of misuse.
20PaymentsWithPaymentCardLocalWeek	This payment card submitted 20 or more payments in the previous week. This is atypical and may be an indicator of misuse.
3CustomerIDsPerDeviceLocalDay	This device has submitted transactions using 3 or more distinct customer IDs in the previous 24 hours. This is abnormal and may be an indicator of a card-testing attack or free-trial abuse.
3CustomerIDsPerDeviceLocalWeek	This device has submitted transactions using 3 or more distinct customer IDs in the previous 7 days. This is abnormal and may be an indicator of a card-testing attack or free-trial abuse.
3DevicesPerCustomerIDLocalDay	Three or more devices have been used to submit transactions with this customer ID in the previous 24 hours. This may be an indicator of misuse.
3DevicesPerCustomerIDLocalWeek	Three or more devices have been used to submit transactions with this customer ID in the previous 7 days. This may be an indicator of misuse.
3DevicesPerEmailGlobalDay	Three or more devices have been used to submit transactions with this email address in the previous 24 hours. This may be an indicator of misuse.
3DevicesPerEmailGlobalWeek	Three or more devices have been used to submit transactions with this email address in the previous 7 days. This may be an indicator of misuse.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
3DevicesPerPaymentCardGlobalDay	Three or more devices have been used to submit transactions with this payment card in the previous 24 hours. This may be an indicator of misuse.
3DevicesPerPaymentCardGlobalWeek	Three or more devices have been used to submit transactions with this payment card in the previous 7 days. This may be an indicator of misuse.
3EmailsPerDeviceGlobalDay	This device has submitted transactions using 3 or more distinct email addresses in the previous 24 hours. This is abnormal and may be an indicator of a card-testing attack or free-trial abuse.
3EmailsPerDeviceGlobalWeek	This device has submitted transactions using 3 or more distinct email addresses in the previous 7 days. This is abnormal and may be an indicator of a card-testing attack or free-trial abuse.
3EmailsPerFuzzyDeviceLocalHour	This device appears to have submitted transactions using 3 or more distinct email addresses in the previous 60 minutes. This is abnormal and may be an indicator of a card-testing attack or free-trial abuse.
3PaymentCardsPerDeviceGlobalDay	This device has submitted transactions using 3 or more distinct payment cards in the previous 24 hours. This is abnormal and may be an indicator of a card-testing attack or free-trial abuse.
3PaymentCardsPerDeviceGlobalWeek	This device has submitted transactions using 3 or more distinct payment cards in the previous 7 days. This is abnormal and may be an indicator of a card-testing attack or free-trial abuse.
3PaymentsOnDeviceLocalHour	This device has submitted 3 or more payments in the previous hour. This is atypical and may be an indicator of misuse.
3PaymentsOnFuzzyDeviceLocalHour	This device appears to have submitted 3 or more payments in the previous hour. This is atypical and may be an indicator of misuse.
3PaymentsOnTrueIPLocalHour	This True IP submitted 3 or more payments in the previous hour. This is atypical and may be an indicator of misuse.
3ProxiesPerDeviceGlobalDay	This device submitted transactions through 3 or more distinct IP proxies in the previous 24 hours. This is atypical and may be an indicator of misuse.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
4ScreenResolutionsPerDeviceGlobalDay	This device has used 4 or more screen resolutions in the past day. This is atypical and may indicate misuse.
5PaymentsOnDeviceLocalDay	This device has submitted 5 or more payments in the previous 24 hours. This is atypical and may be an indicator of misuse.
5PaymentsOnDeviceLocalHour	This device has submitted 5 or more payments in the previous hour. This is atypical and may be an indicator of misuse.
5PaymentsOnFuzzyDeviceLocalDay	This device appears to have submitted 5 or more payments in the previous 24 hours. This is atypical and may be an indicator of misuse.
5PaymentsOnFuzzyDeviceLocalHour	This device appears to have submitted 5 or more payments in the previous hour. This is atypical and may be an indicator of misuse.
5PaymentsOnTrueIPLocalDay	This True IP has submitted 5 or more payments in the previous day. This is atypical and may be an indicator of misuse.
5PaymentsOnTrueIPLocalHour	This True IP submitted 5 or more payments in the previous hour. This is atypical and may be an indicator of misuse.
5PaymentsWithCustomerIDLocalHour	This customer ID submitted 5 or more payments in the previous hour. This is atypical and may be an indicator of misuse.
5PaymentsWithEmailAddressLocalHour	This email address has submitted 5 or more payments in the previous hour. This is atypical and may be an indicator of misuse.
5PaymentsWithPaymentCardLocalHour	This payment card submitted 5 or more payments in the previous hour. This is atypical and may be an indicator of misuse.
50PaymentsOnDeviceLocalWeek	This device has submitted 50 or more payments in the previous week. This is atypical and may be an indicator of misuse.
50PaymentsOnFuzzyDeviceLocalWeek	This device appears to have submitted 50 or more payments in the previous week. This is atypical and may be an indicator of misuse.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
50PaymentsOnTrueIPLocalWeek	This True IP has submitted 50 or more payments in the previous week. This is atypical and may be an indicator of misuse.
AnonymousProxy	This transaction was submitted through an anonymous web proxy, a method that is sometimes employed when trying to cloak one's identity.
AnonymousProxyIP	This transaction was submitted through an anonymous proxy IP Address, a method that is sometimes employed when trying to cloak one's identity.
BINCustomerAddressGeolocationMismatch	The customer's bill-to address country does not match that of the payment card's issuing bank. This may be an indicator of a fraud attack.
ComputerGeneratedEmail	This email address may have been automatically generated by a computer. Fraudsters frequently employ automated bots that create email addresses programmatically to enable their fraud attacks.
CookiesDisabled	The browser used to submit this transaction has disabled cookies. This is common to fraud attacks and may be an indicator of misuse.
CookiesJavascriptDisabled	The browser used to submit this transaction has disabled cookies and JavaScript. This is common to fraud attacks and may be an indicator of misuse.
CustomAttribute1OnLocalBlacklist	Custom attribute 1 for this transaction is on Vantiv's ThreatMetrix-hosted blacklist.
CustomAttribute1OnLocalWhitelist	Custom attribute 1 for this transaction is on Vantiv's ThreatMetrix-hosted whitelist.
CustomAttribute2OnLocalBlacklist	Custom attribute 2 for this transaction is on Vantiv's ThreatMetrix-hosted blacklist.
CustomAttribute2OnLocalWhitelist	Custom attribute 2 for this transaction is on Vantiv's ThreatMetrix-hosted whitelist.
CustomAttribute3OnLocalBlacklist	Custom attribute 3 for this transaction is on Vantiv's ThreatMetrix-hosted blacklist.
CustomAttribute3OnLocalWhitelist	Custom attribute 3 for this transaction is on Vantiv's ThreatMetrix-hosted whitelist.
CustomAttribute4OnLocalBlacklist	Custom attribute 4 for this transaction is on Vantiv's ThreatMetrix-hosted blacklist.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
CustomAttribute4OnLocalWhitelist	Custom attribute 4 for this transaction is on Vantiv's ThreatMetrix-hosted whitelist.
CustomAttribute5OnLocalBlacklist	Custom attribute 5 for this transaction is on Vantiv's ThreatMetrix-hosted blacklist.
CustomAttribute5OnLocalWhitelist	Custom attribute 5 for this transaction is on Vantiv's ThreatMetrix-hosted whitelist.
CustomerIDOnLocalBlacklist	The customer ID for this transaction is on Vantiv's ThreatMetrix-hosted blacklist.
CustomerIDOnLocalWhitelist	The customer ID for this transaction is on Vantiv's ThreatMetrix-hosted whitelist.
CustomerNameOnLocalBlacklist	The customer name for this transaction is on Vantiv's ThreatMetrix-hosted blacklist.
CustomerNameOnLocalWhitelist	The customer name for this transaction is on Vantiv's ThreatMetrix-hosted whitelist.
DeviceCountriesNotAllowed	This transaction originated from an IP address located in a country on Vantiv's ThreatMetrix-hosted blacklist.
DeviceGlobalAgeLessThanOneHour	The originating device was first seen across the entire ThreatMetrix global network within the past hour. This is uncommon and may point to a fraudster simulating a new device through advanced techniques in an attempt to avoid detection.
DeviceIDOnThreatMetrixGlobalBlacklist	The originating device is on the ThreatMetrix global blacklist.
DeviceLocalAgeLessThanOneHour	The originating device was first seen by Vantiv within the past hour. This may point to a fraudster simulating a new device through advanced techniques in an attempt to avoid detection.
DeviceNotFingerprinted	ThreatMetrix could not fingerprint the originating device. This is atypical and may indicate a deliberate attempt by the user to cloak his or her identity.
DeviceOnLocalBlacklist	The originating device is on Vantiv's ThreatMetrix-hosted blacklist.
DeviceOnLocalWhitelist	The originating device is on Vantiv's ThreatMetrix-hosted whitelist.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
DeviceOnThreatMetrixGlobalBlacklist	The originating device is on the ThreatMetrix global blacklist.
DeviceRejectedByNetwork10Times	The originating device has been rejected by one of ThreatMetrix's customers and/or partners 10 or more times on the suspicion of fraud.
DeviceRejectedByNetwork25Times	The originating device has been rejected by one of ThreatMetrix's customers and/or partners 25 or more times on the suspicion of fraud.
DeviceRejectedByNetwork5Times	The originating device has been rejected by one of ThreatMetrix's customers and/or partners 5 or more times on the suspicion of fraud.
DeviceRejectedByNetworkInLastWeek	The originating device has been rejected by one of ThreatMetrix's customers and/or partners in the last week on the suspicion of fraud.
DeviceReviewedByNetwork5Times	The originating device has been reviewed by one of ThreatMetrix's customers and/or partners 5 or more times on the suspicion of fraud.
DeviceReviewedByNetwork10Times	The originating device has been reviewed by one of ThreatMetrix's customers and/or partners 10 or more times on the suspicion of fraud.
DeviceReviewedByNetwork25Times	The originating device has been reviewed by one of ThreatMetrix's customers and/or partners 25 or more times on the suspicion of fraud.
EmailDistanceTraveled	This email address has been associated with transactions originating from locations at least 1,000 miles apart in the last hour. This is a red flag and warrants caution.
EmailHostnameTooLong	The hostname portion (i.e. to the right of "@") of this email address exceeds 30 characters. Email addresses associated with suspicious domain names are often used as part of attacks. Overly long hostnames are a common marker of such domains.
EmailHostnameWithNonLetters	The hostname portion (i.e. to the right of "@") of this email address contains non-letter characters (e.g. numbers and special characters). Email addresses associated with suspicious domain names are often used as part of attacks. Hostnames with non-letter characters are a common marker of such domains.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
EmailOnLocalBlacklist	The customer email address for this transaction is on Vantiv's ThreatMetrix-hosted blacklist.
EmailOnLocalWhitelist	The customer email address for this transaction is on Vantiv's ThreatMetrix-hosted whitelist.
EmailOnThreatMetrixGlobalBlacklist	This email address is on the ThreatMetrix global blacklist.
EmailRejectedByNetwork10TimesInLastDay	The associated email address has been rejected by one of ThreatMetrix's customers and/or partners 10 or more times in the last day on the suspicion of fraud.
EmailRejectedByNetworkInLastWeek	A transaction using this email address has been rejected by one of ThreatMetrix's customers and/or partners in the last week on the suspicion of fraud.
EmailUsernameTooLong	The name portion (i.e. to the left of "@") of this email address exceeds 30 characters. Email addresses associated with suspicious usernames are often used as part of attacks. Overly long usernames are a common marker of such domains.
EmailUsernameWithNonLetters	The name portion (i.e. to the left of "@") of this email address contains non-letter characters (e.g. numbers and special characters). Email addresses associated with suspicious usernames are often used as part of attacks. Usernames with non-letter characters are a common marker of such domains.
ExcessivePaymentsOnDeviceHour	An abnormally high number of transactions have been submitted from this device in the last hour. This is a common indicator of fraudulent payment.
ExcessivePaymentsOnDeviceDay	An abnormally high number of transactions have been submitted from this device in the last 24 hours. This is a common indicator of fraudulent payment.
ExcessivePaymentsOnFuzzyDeviceHour	An abnormally high number of transactions appear to have been submitted from this device in the last hour. This is a common indicator of fraudulent payment.
ExcessivePaymentsOnFuzzyDeviceDay	An abnormally high number of transactions appear to have been submitted from this device in the last 24 hours. This is a common indicator of fraudulent payment.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
FlashBrowserLanguageMismatch	The language used by the web browser used to submit this transaction does not match the language used by the Flash plug-in. This is atypical and may be an indicator of misuse.
FlashCookiesJavascriptDisabled	The browser used to submit this transaction has disabled Flash objects, cookies, and JavaScript. This is common to fraud attacks and may be an indicator of misuse.
FlashCookiesDisabled	The browser used to submit this transaction has disabled Flash objects and cookies. This is common to fraud attacks and may be an indicator of misuse.
FlashDisabled	The browser used to submit this transaction has disabled Flash objects. This is common to fraud attacks and may be an indicator of misuse.
FlashImagesCookiesDisabled	The browser used to submit this transaction has disabled Flash objects, images, and cookies. This is common to fraud attacks and may be an indicator of misuse.
FlashImagesCookiesJavascriptDisabled	The browser used to submit this transaction has disabled Flash objects, images, cookies, and JavaScript. This is common to fraud attacks and may be an indicator of misuse.
FlashImagesDisabled	The browser used to submit this transaction has disabled Flash objects and images. This is common to fraud attacks and may be an indicator of misuse.
FlashImagesJavascriptDisabled	The browser used to submit this transaction has disabled Flash objects, images, and JavaScript. This is common to fraud attacks and may be an indicator of misuse.
FlashJavascriptDisabled	The browser used to submit this transaction has disabled Flash objects and JavaScript. This is common to fraud attacks and may be an indicator of misuse.
FuzzyDeviceLocalAgeLessThanOneHour	The originating device appears to have been seen by Vantiv for the first time within the past hour. This may point to a fraudster simulating a new device through advanced techniques in an attempt to avoid detection.
FuzzyDeviceOnLocalBlacklist	The originating device appears to be on Vantiv's ThreatMetrix-hosted blacklist.
FuzzyDeviceOnLocalWhitelist	The originating device appears to be on Vantiv's ThreatMetrix-hosted whitelist.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
FuzzyDeviceOnThreatMetrixGlobalBlacklist	The originating device appeas to be on the ThreatMetrix global blacklist.
FuzzyDeviceRejectedByNetworkInLastWeek	The originating device appears to have been rejected by one of ThreatMetrix's customers and/or partners in the last week on the suspicion of fraud.
GeolocationLanguageMismatch	The language detected from the originating web browser is not appropriate for the location. This is atypical and may be an indicator of misuse.
HiddenProxy	This transaction was submitted through a hidden web proxy, a method that is sometimes employed when trying to cloak one's identity.
ImagesCookiesDisabled	The browser used to submit this transaction has disabled images and cookies. This is common to fraud attacks and may be an indicator of misuse.
ImagesCookiesJavascriptDisabled	The browser used to submit this transaction has disabled images, cookies, and JavaScript. This is common to fraud attacks and may be an indicator of misuse.
ImagesDisabled	The browser used to submit this transaction has disabled images. This is common to fraud attacks and may be an indicator of misuse.
ImagesJavascriptDisabled	The browser used to submit this transaction has disabled images and JavaScript. This is common to fraud attacks and may be an indicator of misuse.
IPHasNegativeReputation	The originating IP address is a potential threat based upon analysis of its activity across the ThreatMetrix network.
IPOnLocalBlacklist	The originating IP address is on Vantiv's ThreatMetrix-hosted blacklist.
IPOnLocalWhitelist	The originating IP address is on Vantiv's ThreatMetrix-hosted whitelist.
IPOnThreatMetrixGlobalBlacklist	The originating IP address is on the ThreatMetrix global blacklist.
IPRejectedByNetwork10Times	The originating IP address has been rejected by one of ThreatMetrix's customers and/or partners 10 or more times on the suspicion of fraud.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
IPRejectedByNetwork25Times	The originating IP address has been rejected by one of ThreatMetrix's customers and/or partners 25 or more times on the suspicion of fraud.
IPRejectedByNetwork5Times	The originating IP address has been rejected by one of ThreatMetrix's customers and/or partners 5 or more times on the suspicion of fraud.
JavascriptDisabled	The browser used to submit this transaction has disabled JavaScript. This is common to fraud attacks and may be an indicator of misuse.
KnownVPNISP	This transaction was submitted through a known Virtual Private Network (VPN), a method that is sometimes employed when trying to cloak one's identity.
MalwareDetectedOnDevice	The originating device appears have to been infected with malware.
OpenProxy	This transaction was submitted through an open web proxy, a method that is sometimes employed when trying to cloak one's identity.
PaymentCardBINShippingAddressGeolocationMismatch	The customer's ship-to address country does not match that of the payment card's issuing bank. This may be an indicator of a fraud attack.
PaymentCardBINTrueIPGeolocationMismatch	The geolocation of the True IP address does not match that of the payment card's issuing bank. This may be an indicator of a fraud attack.
PaymentCardDistanceTraveled	This payment card has been associated with transactions originating from locations at least 1,000 miles apart in the last hour. This is a red flag and warrants caution.
PaymentCardOnThreatMetrixGlobalBlacklist	This payment card is on the ThreatMetrix global blacklist.
PaymentCardRejectedByNetworkInLastWeek	A transaction using this payment card has been rejected by one of ThreatMetrix's customers and/or partners in the last week on the suspicion of fraud.
PhoneNumberOnLocalBlacklist	The customer telephone number for this transaction is on Vantiv's ThreatMetrix-hosted blacklist.
PhoneNumberOnLocalWhitelist	The customer telephone number for this transaction is on Vantiv's ThreatMetrix-hosted whitelist.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
PossibleCookieWipingDay	The user appears to have cleared his or her browser's cookies 3 or more times in the last day. This is common to fraud attacks and may be an indicator of misuse.
PossibleCookieWipingHour	The user appears to have cleared his or her browser's cookies 3 or more times in the last hour. This is common to fraud attacks and may be an indicator of misuse.
PossibleCookieWipingWeek	The user appears to have cleared his or her browser's cookies 3 or more times in the last week. This is common to fraud attacks and may be an indicator of misuse.
PossibleVPNOrTunnel	This transaction may have been submitted through a Virtual Private Network (VPN), a method that is sometimes employed when trying to cloak one's identity.
PossibleVPNConnection	This transaction may have been submitted through a Virtual Private Network (VPN), a method that is sometimes employed when trying to cloak one's identity.
PotentialVirtualMachine	This transaction may have been submitted using a Virtual Machine, a method that is sometimes employed when trying to cloak one's identity.
ProxyHasNegativeReputation	The originating IP proxy is a potential threat based upon an analysis of its activity across the ThreatMetrix network.
ProxyIPHasNegativeReputation	The originating IP address is a potential threat based upon analysis of its activity across the ThreatMetrix network.
ProxyIPOnLocalBlacklist	The originating proxy IP address is on Vantiv's ThreatMetrix-hosted blacklist.
ProxyIPOnLocalWhitelist	The originating proxy IP address is on Vantiv's ThreatMetrix-hosted whitelist.
ProxyIPOnThreatMetrixGlobalBlacklist	The originating proxy IP address is on the ThreatMetrix global blacklist.
SatelliteISP	This transaction was submitted through a Satellite Internet Service Provider, a method that is sometimes employed when trying to cloak one's identity.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
SatelliteProxyISP	This transaction was submitted through a Satellite Proxy Internet Service Provider, a method that is sometimes employed when trying to cloak one's identity.
SessionAnomaly	Characteristics of the originating device appear to have been modified during the course of the user's web session. This is atypical and may indicate misuse.
ShippingAddressTrueIPGeolocationMismatch	The shipping address country does not match that of the True IP address. This may be an indicator of a package redirection/interception/forwarding or re-shipping fraudster attack.
SuspectedSessionCloaking	The characteristics of the originating browser are consistent with common fraud attacks, and may be an indicator of a fraudster's deliberate attempt to cloak his or her identity.
SuspectedTORNetwork	This transactions appears to have originated from a TOR network, a common source of fraud attacks.
SystemStateAnomaly	The system state of the originating device has changed two or more times within the past hour. This is atypical and may indicate misuse.
TimeZoneTrueGeolocationMismatch	The time zone setting on the originating device does not match to the true geolocation of the customer. This is atypical and may be an indicator of misuse.
TransparentProxy	This transaction was submitted through a transparent web proxy, a method that is most often used in corporate environments, though also employed when trying to cloak one's identity.
TrueIPDNSGeolocationMismatch	The geolocation of the True IP address does not match that of the DNS provider. This may be an indicator of a fraudster's attempt to cloak his or her identity.
TrueIPHasNegativeReputation	The originating IP address is a potential threat based upon analysis of its activity across the ThreatMetrix network.
TrueIPOnLocalBlacklist	The originating true IP address is on Vantiv's ThreatMetrix-hosted blacklist.
TrueIPOnLocalWhitelist	The originating true IP address is on Vantiv's ThreatMetrix-hosted whitelist.

TABLE 6 Advanced Fraud Tools Triggered Rules

Triggered Rule Name	Description
TrueIPOnThreatMetrixGlobalBlacklist	The originating true IP address is on the ThreatMetrix global blacklist.
TrueIPProxyIPCityMismatch	The city of the True IP address does not match that of the Proxy IP address. This may be an indicator of a fraudster's attempt to cloak his or her identity.
TrueIPProxyIPGeolocationMismatch	The geolocation of the True IP address does not match that of the Proxy IP address. This may be an indicator of a fraudster's attempt to cloak his or her identity.
TrueIPProxyIPISPMismatch	The Internet Service Provider of the True IP address does not match that of the Proxy IP address. This may be an indicator of a fraudster's attempt to cloak his or her identity.
TrueIPProxyIPOrganizationMismatch	The organization of the True IP address does not match that of the Proxy IP address. This may be an indicator of a fraudster's attempt to cloak his or her identity.
TrueIPProxyIPRegionMismatch	The region of the True IP address does not match that of the Proxy IP address. This may be an indicator of a fraudster's attempt to cloak his or her identity.
TrueIPRejectedByNetwork10TimesInLastDay	The orignating IP address has been rejected by one of ThreatMetrix's customers and/or partners 10 or more times in the last day on the suspicion of fraud.
TrueIPRejectedByNetworkInLastWeek	The originating true IP has been rejected by one of ThreatMetrix's customers and/or partners in the last week on the suspicion of fraud.
UnusualProxyAttributes	This web proxy used to submit the transaction has unusual attributes (e.g. dialup), which may indicate an attempt to cloak one's identity.

ACH Return Reason Codes

Table 7 lists the ACH Return Reason codes, which can apply to either eCheck transactions or Dynamic Payout funding instructions. These codes are visible in iQ on the eCheck Returns Received report, as well as the Transaction Detail screen and the Funding Instruction Detail screen, however they are not returned in LitleXML response messages.

NOTE: **If an eCheck is returned for reason Code R01 or R09, it is eligible for redeposit.**

TABLE 7 ACH Return Reason Codes

ACH Return Reason Code	Description
R01	Insufficient funds in account
R02	Account is closed
R03	No account on file
R04	Invalid account number
R05	Unauthorized debit to consumer account
R06	Returned at request of ODFI
R07	Authorization revoked by customer
R08	Payment stopped
R09	Insufficient collected funds in account being charged
R10	Customer advises not Authorized, notice not provided, improper source document, or amount of entry not accurately obtained from source document
R11	Check truncation return
R12	Account sold to another financial institution
R13	Invalid ACH routing number
R14	Representative payee is deceased or cannot continue in that capacity
R15	Beneficiary or account holder other than representative payee deceased
R16	Account funds have been frozen
R17	Item returned because of invalid data; refer to addenda fro information
R18	Improper effective date
R19	Amount error
R20	Account does not allow ACH transactions or limit for transactions has been exceeded
R21	Invalid company identification
R22	Invalid individual ID

TABLE 7 ACH Return Reason Codes

ACH Return Reason Code	Description
R23	Credit entry refused by receiver
R24	Duplicate entry
R25	Addenda record error
R26	Mandatory field error
R27	Trace number error
R28	Routing/transit number check digit error
R29	Corporate customer advised not authorized
R30	RDFI not participant in check truncation program
R31	Permissible return entry
R32	RDFI non-settlement
R33	Return of item
R34	Limited participation ODFI
R35	Return of improper debit entry
R36	Return of improper credit entry
R37	Source document presented for payment
R38	Stop payment on source document
R39	Improper source document
R40	Return of item by government agency
R41	invalid Transaction Code
R42	Routing/transit number check digit error
R43	Invalid account number
R44	Invalid individual ID
R45	Invalid individual name or company name
R46	Invalid representative payee indicator code
R47	Duplicate enrollment
R50	State law affecting RCK acceptance

TABLE 7 ACH Return Reason Codes

ACH Return Reason Code	Description
R51	Item is ineligible, notice not provided, signature not genuine, or original item altered for adjustment entry
R52	Stop payment on item
R53	Item and ACH entry presented for payment
R61	Misrouted return - RDFI for original entry has placed incorrect routing/transit number in RDFI identification field
R67	Duplicate return
R68	Untimely return - return was not sent within the established time frame
R69	Field errors
R70	Permissible return entry not accepted
R71	Misrouted dishonored return -incorrect routing/transit number in RDFI identification field
R72	Untimely return - dishonored return was not sent within the established timeframe
R73	Timely original return - RDFI certifies the original return entry was sent within established timeframe for original returns
R74	Corrected return - RDFI is correcting a previous return entry that was dishonored because it contained incomplete or incorrect information
R75	Original return not a duplicate
R76	No errors found
R80	Cross-border payment coding error
R81	Non-participant in cross-border program
R82	Invalid foreign RDFI identification
R83	Foreign RDFI unable to settle
R84	Cross-border entry not processed by originating gateway operator
R94	Administrative return item was processed and resubmitted as a photocopy
R95	Administrative return item was processed and resubmitted as a MICR-Split
R97	Administrative return item was processed and resubmitted with corrected dollar amount

TABLE 7 ACH Return Reason Codes

ACH Return Reason Code	Description
R98	Indicates a return PAC (pre-authorized check); RDFI provides a text reason and indicated a new account number on the PAC itself
R99	Indicates a return PAC (pre-authorized check); RDFI provides a text reason on the PAC itself for which there is no equivalent return reason code

ACH Notice of Change (NOC) Codes

Table 8 lists the ACH NOC Change Codes, which can apply to either eCheck transactions or Dynamic Payout funding instructions. These codes are included in the daily NOC report made available to you via sFTP, as well as the Transaction Detail screen and the Funding Instruction Detail screen.

TABLE 8 ACH Notice of Change (NOC) Codes

ACH NOC Change Code	Description
C01	Incorrect account number
C02	Incorrect routing/transit number
C03	Incorrect routing/transit number and incorrect account number
C04	Incorrect account name
C05	Incorrect transaction code
C06	Incorrect account number and transaction code
C07	Incorrect routing/transit number, account number and transaction code
C08	Incorrect foreign RDFI identification
C09	Incorrect individual ID
C13	Addenda format error
C61	Misrouted NOC
C62	Incorrect trace number
C63	Incorrect company ID

TABLE 8 ACH Notice of Change (NOC) Codes

ACH NOC Change Code	Description
C64	Incorrect individual ID
C65	Incorrectly formatted correct data
C66	Incorrect discretionary data
C67	Routing/transit number not from original entry
C68	Account number not from original entry
C69	Incorrect transaction code
C96	Administrative return dishonor (dollar amount will be zero)
C99	Converted to MICR draft (check conversion items)