



BluePay 2.0 Daily Report V2 Interface

BluePay Reporting API Documentation

Reference Guide

February 2025

© 2024-2025 Fiserv, Inc. or its affiliates. Fiserv is a trademark of Fiserv, Inc., registered or used in the United States and foreign countries, and may or may not be registered in your country. All trademarks, service marks and trade names referenced in this material are the property of their respective owners.

<http://www.fiserv.com>

This document is classified as Fiserv Public.

Content

- About this Document** **4**
 - Intended Audience 4
 - Assistance & Feedback 4
- Overview** **5**
 - URL 5
 - Input Format 5
 - Output Format 5
 - Sample Request and Response 6
 - Request Format 6
 - Response Format 6
 - Error Responses 8
- Input Fields** **9**
 - Aggregate Fields 12
 - Miscellaneous Filters 12
- Output Fields** **18**
 - Merchant Information 18
 - Transaction Information 19
 - Transaction Response Information 22
 - Credit Card Payment Information 26
 - ACH Payment Information 29
 - Customer Information 31
 - Additional Transaction Information 33
- Appendix I - Tamper Proof Seals** **36**
 - TPS Hash Types 36
 - Calculating the Tamper Proof Seal 36

STEP 1: Build the pre-hash string	36
STEP 2: Perform the Hash	37
To calculate the TAMPER_PROOF_SEAL, merchant 'A' can perform the following steps	38
STEP 1:	38
STEP 2:	38
Appendix II - Quick Response Field Reference	39
Revision History	42

About this Document

This documentation provides technical guidance to the users accessing the reporting interface for the retrieval of transaction data.

Intended Audience

This document is written for merchants, partners, and developers who will be responsible for integrating payment processing functionality with the BluePay Payment Gateway. This document provides specification on BluePay Gateway reporting API.

Assistance & Feedback

Use the following contact information for help with the BluePay Payment Gateway integration or to provide feedback on this document.

Support Level	Contact Details
BluePay Integration Support Team	bluepay-integration@fiserv.com

Support hours are Monday through Friday 8:00am to 5:00pm (CST UTC-6).

Overview

The “bpdailyreport2” is the reporting interface that retrieves transaction history based on search criteria, such as date range.

URL

The API endpoint is as follows:

```
https://secure.bluepay.com/interfaces/bpdailyreport2
```

Input Format

This web service takes the input as the standard HTTP "POST" request. The parameters to the service are URI-encoded in the body of the request.

Output Format

This web service returns the output as the standard HTTP response format with header and body of the response separated by an empty line. The header contains the standard HTTP response status codes. For example, 200 indicates a success and 400 indicates an error or other request failure.

- If successful, the response body contains comma-separated transaction data.
- If failed, the output contains a single line, containing an error message that displays the reason for failure.

Except for the [DO_NOT_ESCAPE](#) option used, existing commas within the transaction data are preceded by a backslash (“\”) character. Commas “,” becomes backslash commas “\\”.

Sample Request and Response

Use the following fields to run the API:

- Request method: POST
- Requested URL: <https://secure.bluepay.com/interfaces/bpdailyreport2>
- Content-Type: application/x-www-form-urlencoded

Request Format

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 292
Host: secure.bluepay.com
User-Agent: TransactionProcessingApplication
Accept: */*
ACCOUNT_ID=100009229785&REPORT_START_DATE=2023-01-17%2000%3A00%
3A00&REPORT_END_DATE=2023-01-19%2000%3A00%3A00&MODE=TEST&TPS_
HASH_TYPE=HMAC_SHA512&TAMPER_PROOF_SEAL=456b25c0f6b001a6c22d4ae
1a05b81c25fca3c3d3bb0ea5f8437b9d33f8c17fecc730d3c5d0c5b52f4bf2339b34cc0
06 e8b98c92e039feeafda688aadcd1d2d04
```


Response Format

```
Date: Fri, 04 Feb 2023 15:35:20 GMT
Content-Type: text/html; charset=ISO-8859-1
Transfer-Encoding: chunked
Connection: keep-alive
X-item-count: 2
Vary: Accept-Encoding
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800,report-uri=https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct
X-Content-Type-Options: nosniff
Server: cloudflare
CF-RAY: 6d84f7df0d1d8108-ORD
```

```
"id","payment_type","trans_type","amount","card_type","payment_account","order_
id","
invoice_id","custom_id","custom_id2","master_id","status","f_void","message","origin
","issue_date","settle_date","rebilling_id","settlement_id","card_expire","bank_name
","addr1","addr2","city","state","zip","phone","email","auth_
code","name1","name2","
company_name","memo","backend_id","doc_type","f_captured"
```

```
"101233145802","CREDIT","SALE","1.00","VISA","xxxxxxxxxxxxx1111","101203057676
","101203057676","","","101219299271","1","","Approved Sale","BATCH","2023-01-
1808:28:13","2023-01-1902:24:08","","101233547902","1227","","
25WRandolphSt","Apt1720","Chicago","IL","60601","6303002365","
John.Doe@Fiserv.com","ALVSGO","John","Dooe","Fiserv, Inc.,"","262578219586","",""
```

```
"101233170130","CREDIT","SALE","1.00","VISA","xxxxxxxxxxxxx1111","101233170130
","1012 33170130","","","1","","Approved Sale","BATCH","2023-01-18
09:23:53","2023-01-19
02:24:08","","101233547902","1225","","","","","","","ZJUDQD","","","5999098
03219","",""
```

 To understand the step-wise calculation of the Tamper Proof Seal, refer to the [Appendix-I](#) section.

Error Responses

An unsuccessful request returns a response with the HTTP error code "400 Bad Request." The cause of the error is included in the body of the response. It gives a brief description of the error.

The following table lists some of the common error messages.

Message	Description	Example
"Security Error"	Issue related to authentication, permissions, or some other security check.	"SECURITY ERROR"
"Missing" + an INPUT PARAMETER	Required field is missing. If the field is included in the request, it may have been incorrectly formatted.	"Missing ACCOUNT_ID"
ACCOUNT_ID or PLATFORM_MERCHANT_ID	Both parameters were provided. Use one parameter.	"ACCOUNT_ID or PLATFORM_MERCHANT_ID is required."



Contact the [BluePay Integration team](#) to get assistance in resolving any errors.

Input Fields

The following input fields are used to fetch the daily transaction report


ACCOUNT_ID	
Required:	Unless PLATFORM_MERCHANT_ID is included.
Description:	The BluePay-assigned account number associated with the current reporting request.
Maximum Length:	12


PLATFORM_MERCHANT_ID	
Required:	Unless ACCOUNT_ID is included.
Description:	The platform Merchant ID associated with the current reporting request.
Maximum Length:	20

REPORT_START_DATE, REPORT_END_DATE	
Required:	Yes
Description:	Date and time span for which you want to retrieve the transaction history. Pass the date and time (start and end) values, in the YYYY-MM-DD HH:MM:SS format.
Example:	To get the list of all the statuses updated on 2021-08-08, set the REPORT_START_DATE to 2021-08-08 00:00:00 and REPORT_END_DATE to 2021-08-08 23:59:59

RESPONSEVERSION	
Required:	No
Description:	Version related to response fields. If not set, response contains only the version 1 (RESPONSEVERSION 1) fields.
Default:	1
Latest:	15


TAMPER_PROOF_SEAL	
Required:	Yes

TAMPER_PROOF_SEAL	
Description:	Hash for security. Compute the Tamper Proof Seal as follows: <div style="border: 1px solid gray; padding: 5px; width: fit-content; margin: 10px auto;"> Hash (The Merchant's Secret Key + ACCOUNT_ID + REPORT_START_DATE + REPORT_END_DATE) </div>
<div style="border: 1px solid blue; padding: 10px;"> <p> In the hex format, '+' represents string concatenation and the field names represent the contents of the respective fields or "" (empty string with no space) if empty or unsent. For more information, refer to the Appendix-I section.</p> </div>	

TPS_DEF	
Required:	No
Description:	Space-separated list of input field names in the exact order they are to be used for calculating the TAMPER_PROOF_SEAL. If not set or blank, TPS_DEF defaults to: <div style="border: 1px solid gray; padding: 5px; width: fit-content; margin: 10px auto;"> TPS_DEF= "ACCOUNT_ID PLATFORM_MERCHANT_ID REPORT_START_DATE REPORT_END_DATE" </div>
<div style="border: 1px solid blue; padding: 10px;"> <p> The Merchant's Secret Key is always used in the calculation of the TAMPER_PROOF_SEAL but should not be included in the TPS_DEF.</p> </div>	

DO_NOT_ESCAPE	
Required:	No
Description:	Flag value that indicates whether to remove all commas and quotes from the output data and retrieve only comma-separated results.
Values:	0 or 1
Default:	0

RESPONSEVERSION	
Required:	No
Description:	Version related to response fields. If not set, response contains only the version 1 (RESPONSEVERSION 1) fields.
Latest:	15
Default:	1

QUERY_BY_SETTLEMENT	
Required:	No
Description:	Fetches the report based on the settlement date. By default, the bpdailyreport2 queries by the transaction date, also known as the issue date. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  By using this option, you receive only the settled transactions in the output and not any authorization or void details in the output. </div>
Values:	0 or 1
Default:	0

QUERY_BY_HIERARCHY	
Required:	No
Description:	Flag that indicates to include child accounts in the output. The account_id field is returned in the output as the last column, regardless of RESPONSEVERSION .
Values:	0 or 1
Default:	0

EXCLUDE_ERRORS	
Required:	No
Description:	Flag that indicates to include only approvals and declines and remove any errors from the report. As billing is not done for error transactions, this parameter returns the exact count as our billing numbers.
Values:	0 or 1
Default:	0

MODE	
Required:	No
Description:	Limits transactions returned to either LIVE or TEST transactions. Live transactions actually moved funds and the Test transactions have a simulated response.
Values:	LIVE or TEST
Default:	LIVE

Aggregate Fields

You can request to view an aggregated report instead of a detailed report. When you use the aggregation fields, the output displays count of transactions, sum of their amounts along with other selected columns.

AGG_QUERY	
Required:	No
Description:	Flag value that indicates whether the aggregation feature is enabled or not. To enable the aggregation reporting feature, set the value to '1'
Valid Values:	0 or 1
Default:	0

AGG_FIELDS	
Required:	Optional
Description:	Space separated list of fieldnames. You cannot aggregate fields by "id" or "amount"
Example:	After URI-Encoding, "AGG_FIELDS=payment_type%20trans_type%20card_type"
Default:	N/A

Miscellaneous Filters

Use the additional filters to retrieve a subset of transactions or to filter the results to fit your purpose. Also, a few filters support searching for blank values by submitting a key without a value.

For example, "KEY="

COMPANY_NAME	
Required:	N/A
Description:	Filter transactions with a specific company name.
Maximum Length:	64
Example:	To search transactions for a company, "abcxyz", apply filters COMPANY_NAME="abcxyz"

FIRST_NAME	
Required:	N/A
Description:	Filter transactions with a specific first name.
Maximum Length:	32
Example:	To filter transactions with the first name, "abc", apply filters FIRST_NAME="abc"

LAST_NAME	
Required:	N/A
Description:	Filter transactions with a specific last name.
Maximum Length:	32
Example:	To filter transactions with the last name, "xyz", apply filters LAST_NAME="xyz"

EMAIL	
Required:	N/A
Description:	Filter transactions with a specific email address.
Maximum Length:	128
Example:	To filter transactions with an email address, apply filters "EMAIL=username%40mail.com"

ORIGIN	
Required:	N/A
Description:	Filter transactions based on the API or BluePay service, from which the transactions were originally initiated.
Valid Values:	<p>The valid values are:</p> <ul style="list-style-type: none"> • "bp10emu" • "bp20post" • "asbyemu" • "a.net-aim" • "REJECT" • "FIXER" • "PAYOUT" • "REBILL" • "AGG" • "BATCH" • "CAPQUEUE" • "FRAUDSCRUB" • "IVR" • "VTerm"
Example:	Filter transactions from bp10emu "ORIGIN=bp10emu"

TRANSACTION_ID	
Required:	N/A
Description:	Filter transactions with a specific email address.
Maximum Length:	12
Example:	To filter transactions with a transaction ID, apply filters "TRANSACTION_ID=100000123456"

MASTER_ID	
Required:	N/A
Description:	Filter transactions based on a specific master ID or a transaction ID token.
Maximum Length:	12
Example:	To filter transactions with the Master ID, apply filters "MASTER_ID=100000123456"

REBILLING_ID	
Required:	NA
Description:	Filter transactions by the Rebilling ID.
Maximum Length:	12
Example:	To filter transactions with the Rebill ID ", apply filters "REBILLING_ID=100000123456"

SETTLEMENT_ID	
Required:	N/A
Description:	Filter transactions by the transaction's settlement ID.
Maximum Length:	12
Example:	To filter transactions with the Settlement ID ", apply filters "SETTLEMENT_ID=100000123456"

PROCESSOR_ID	
Required:	N/A
Description:	Filter transactions by the processor ID.
Maximum Length:	12

PROCESSOR_ID	
Example:	To filter transactions by the Processor ID "", apply filters "PROCESSOR_ID=100000123456"

STATUS	
Required:	N/A
Description:	Search transactions by the transaction status.
Valid Values:	You can pass one of the following values: <ul style="list-style-type: none"> • For Approved, "1" • For Declined, "0" • For Error, "E"
Example:	To fetch all the approved transactions, apply the filter "STATUS=1"

TRANS_TYPE	
Required:	N/A
Description:	Search transactions by transaction type.
Valid Values:	You can pass one of the following values: <ul style="list-style-type: none"> • AUTH • VOID • SALE • CAPTURE • REFUND • CREDIT • UPDATE
Example:	To fetch all the sale transactions, apply the filter "TRANS_TYPE=SALE"

PAYMENT_TYPE	
Required:	N/A
Description:	Search transactions payment type.
Valid Values:	You can pass one of the following values: <ul style="list-style-type: none"> • CREDIT • ACH • SEPA (Single Euro Payments Area)
Example:	To fetch all the transactions by the Credit Card payment mode, apply the filter "PAYMENT_TYPE=CREDIT"

CARD_TYPE	
Required:	N/A
Description:	Fetch the transactions by the card type.
Valid Values:	<p>The valid values are:</p> <ul style="list-style-type: none"> • VISA • MC • DISC • DCCB • JCB • ENRT • AMEX • ACH • BNKC • SWTC • SOLO
Example:	To fetch all the VISA Transactions, apply the filter "CARD_TYPE=VISA"

CARD_PRESENT	
Required:	N/A
Description:	Fetch the transactions based on a flag value (card present or card not present).
Valid Values:	<p>You can pass one of the following values:</p> <ul style="list-style-type: none"> • To search a transaction without the card present, enter "0" • To search a transaction with the card present, enter "1"
Example:	To fetch all the transactions with a credit card present, apply the filter "CARD_PRESENT=1"

CUSTOM_ID	
Required:	N/A
Description:	Filter transactions by the custom ID.
Maximum Length:	16
Example:	To filter transactions with the custom ID, apply filters "CUSTOM_ID=abc"

CUSTOM_ID2	
Required:	N/A
Description:	Filter transactions by the second custom ID.
Maximum Length:	64
Example:	To filter transactions with the custom ID, apply filters "CUSTOM_ID2=abc"

ORDER_ID	
Required:	N/A
Description:	Filter transactions by the order ID.
Maximum Length:	128
Example:	To filter transactions with the order ID, apply filters "ORDER_ID=abc"

INVOICE_ID	
Required:	N/A
Description:	Filter transactions by the invoice ID.
Maximum Length:	64
Example:	To filter transactions with the invoice ID, apply filters "INVOICE_ID=100234567654442"

BACKEND_ID	
Required:	N/A
Description:	Filter transactions by the backend ID.
Maximum Length:	64
Example:	To search for transactions with a specific backend ID, enter "BACKEND_ID=100000123456"

AUTH_CODE	
Required:	N/A
Description:	Filter transactions by a specific authorization code.
Maximum Length:	8
Example:	To search for transactions with a specific bank authorization code, enter "AUTH_CODE=abc123"

AMOUNT	
Required:	N/A
Description:	Filter transactions by a specific transaction amount associated with the current transaction.
Maximum Length:	9
Example:	To search for \$100 transactions, enter "Amount=100.00"

Output Fields

The output fields are displayed as per response version. By default, you can see the limited output fields defined in the RESPONSEVERSION 1. Set RESPONSEVERSION to higher values to receive additional data.

If the requested [RESPONSEVERSION](#) is greater than the default, the output includes all the fields defined for that version, including fields from the lower versions.


For example, if the requested version is RESPONSEVERSION 3, the output fields will include all the fields defined in the response versions 1, 2 and 3.



To view all the response fields and include future updates, set the Response Version to an arbitrarily high value (for example "99"). If you do not want the response data to change as new versions are.

Merchant Information

This section contains the response fields related to gateway account on which the merchant transaction is processed.

account_id	
Description:	12-digit BluePay 2.0 Account ID.
Maximum Length:	12
Response Version:	1 or higher
<div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;">  This field displays only when QUERY_BY_HIERARCHY is set as "1" and it will always display as the last column regardless of RESPONSEVERSION. </div>	

platform_merchnat_id	
Description:	The platform merchant id associated with the transaction.
Maximum Length:	20
Response Version:	18 or higher

account_name	
Description:	Merchant's BluePay Gateway account name.
Maximum Length:	12
Response Version:	9 or higher

owner_id	
Description:	Unique ID number of the user associated with the transaction. The transactions that are processed using an API display the default BluePay account user.
Response Version:	9 or higher

connected_ip	
Description:	Merchant's BluePay Gateway account name.
Maximum Length:	15
Response Version:	4 or higher

Transaction Information

This section contains the response fields related to gateway account on which the transaction is processed:

mode	
Description:	The mode associated with the transactions.
Valid Value:	Valid values are LIVE or TEST
Maximum Length:	4
Response Version:	9 or higher

origin	
Description:	Origination source of the transactions.
Valid Value:	<p>The valid values are:</p> <ul style="list-style-type: none"> • "bp10emu": Post and Redirect API • "bp20post": Post API • "asbyemu": AssureBuy Emulation/XML • "a.net-aim": Authorize.net Emulator • "VTerm": Virtual Terminal • "AGG": Aggregation System • "BATCH": File Upload • "FRAUDSCRUB": Fraud Management System • "REBILL": Recurring Billing System • "REJECT": Automatic reject or chargeback from the bank
Maximum Length:	16
Response Version:	1 or higher

issue_date	
Description:	Timestamp (date and time) when the transaction entered in the BluePay system. The timestamp format is "YYYY-MM-DD HH:MM:SS"
Example:	The sample issue date is "2020-10-05 04:37:00"
Maximum Length:	19
Response Version:	1 or higher

trans_type	
Description:	Transaction type for the current transaction.
Valid Value:	The valid values are: <ul style="list-style-type: none"> • AUTH • VOID • SALE • CAPTURE • REFUND • CREDIT • UPDATE
Maximum Length:	8

payment_type	
Description:	Type of payment.
Valid Value:	The valid values are: <ul style="list-style-type: none"> • "ACH" for Automated Clearing House transactions • "SEPA" for Single Euro Payments Area transactions • "CREDIT" for credit card transactions
Maximum Length:	8
Response Version:	1 or higher

payment_account	
Description:	Payment account used for the transaction. <ul style="list-style-type: none"> • For "CREDIT" transactions, the API masks all the preceding account digits with "x" and displays only the last-four account digits. • For "ACH" transactions, the API returns the payment account in the following format "<account type>:<routing number><x's and last four digits of the account number>"

payment_account	
Example:	<ul style="list-style-type: none"> For credit card transactions, for a 16-digit account number, the payment account displays, "xxxxxxxxxxxx1111" For check transactions (ACH), the payment account displays "C:123123123:xxxxxx4321," where "C" stands for Checking account and S stands for Savings account.
Maximum Length:	32
Response Version:	1 or higher

amount	
Description:	Transaction amount
Maximum Length:	9
Response Version:	1 or higher

amount_tip	
Description:	Tip (monetary amount) paid for this transaction.
Maximum Length:	9
Response Version:	10 or higher

master_id	
Description:	Master transaction ID or token transaction ID.
Maximum Length:	64
Response Version:	1 or higher

rebilling_id	
Description:	ID of the recurring billing schedule that initiated the transaction.
Maximum Length:	12
Response Version:	1 or higher

f_corporate	
Description:	Flag that indicates if the transaction is a corporate transaction or a personal transaction.

f_corporate	
Valid Values:	Possible values are: <ul style="list-style-type: none"> • 1: If the transaction is a corporate transaction • 0: If the transaction is not a corporate transaction
Maximum Length:	1
Response Version:	9 or higher

Transaction Response Information

This section contains the transaction response information fields related to gateway account.

id	
Description:	12-digit transaction ID assigned to a transaction by BluePay.
Maximum Length:	12
Response Version:	1 or higher

status	
Description:	Flag value that indicates transaction status.
Valid Values:	The valid values are: <ul style="list-style-type: none"> • For Approved, "1" • For Declined, "0" • For Error, "E"
Maximum Length:	1
Response Version:	1 or higher

message	
Description:	A short description of the transaction result.
Maximum Length:	64
Response Version:	1 or higher

bank_name	
Description:	Bank name associated with the payment method.
Maximum Length:	64
Response Version:	1 or higher

processor_id	
Description:	ID of the payment configuration that processed the transaction.
Maximum Length:	12
Response Version:	8 or higher

backend_id	
Description:	<ul style="list-style-type: none"> For credit card transactions, this is a transaction tracking number issued by the credit card processing network For Third Party Sender ACH (TPS), it is the funding event ID
Maximum Length:	2048
Response Version:	1 or higher

settlement_id	
Description:	Settlement ID for the transaction.
Maximum Length:	12

settle_date	
Description:	Date and time for the settlement of the transaction. The date format is "YYYY-MM-DD HH:MM:SS"
Example:	The sample settlement date is "2020-11-05 08:37:00"
Maximum Length:	19
Response Version:	1 or higher

f_captured	
Description:	Flag value to identify if a transaction is captured. It applies only to authorization (AUTH) transactions.
Maximum Length:	1
Response Version:	1 or higher

f_refunded	
Description:	Flag value to identify if a transaction was refunded.
Maximum Length:	1
Response Version:	8 or higher

f_void	
Description:	Flag value to identify if the transaction was voided.
Valid Values:	Possible values are: <ul style="list-style-type: none"> • "null", for transactions that are not voided • "1", for transactions that are voided
Maximum Length:	1
Response Version:	1 or higher

f_rebill_master	
Description:	Flag value that indicates if this transaction is the master transaction of a recurring billing schedule.
Valid Values:	Possible values are: <ul style="list-style-type: none"> • 1: True • 0: False
Maximum Length:	1
Response Version:	9 or higher

f_will_capture	
Description:	Flag value to indicate if the transaction was auto-captured.
Valid Values:	Possible values are: <ul style="list-style-type: none"> • 1: True • 0: False
Maximum Length:	1
Response Version:	9 or higher

f_unheld	
Description:	Flag value to indicate if the transaction was on hold or not.
Valid Values:	Possible values are: <ul style="list-style-type: none"> • 0: If the transaction is never on hold • 1: If the transaction initially is on hold, but later released or declined
Maximum Length:	1
Response Version:	9 or higher

unhold_id	
Description:	Original transaction ID before the transaction was put on hold.
Maximum Length:	12
Response Version:	9 or higher

f_transarmor	
Description:	Flag value to indicate if a TransArmor token was used.
Valid Values:	Possible values are: <ul style="list-style-type: none">• 0 or NULL if a TransArmor token was used• 1 if a TransArmor token was used
Maximum Length:	1
Response Version:	11 or higher

Credit Card Payment Information

This section contains the Credit Card Payment information fields related to gateway account.

auth_code	
Description:	Contains the credit card authorization code in the case of a successful transaction. This field displays the reject code on voids created from ACH rejection notices.
Maximum Length:	8
Response Version:	1 or higher

card_type	
Description:	Type of card network.
Valid Values:	<p>The valid values are:</p> <ul style="list-style-type: none"> • "ACH": Automated Clearing House (only for ACH transactions) • AMEX": American Express • "MC": Master Card • "DISC": Discover • "VISA": Visa • "JCB": JCB Co. (formerly known as Japan Credit Bureau) • "DCCB": Diner's Club or Carte Blanche • "ENRT": EnRoute • "BNKC": BankCard • "SWTC": Switch • "SOLO": Solo
Maximum Length:	4
Response Version:	1 or higher

card_expire	
Description:	Credit card expiration date in the MMY format.
Example:	If the expiration date of a credit card is November 2026, the response displays "1126"
Maximum Length:	4
Response Version:	1 or higher

card_present	
Description:	Flag value that checks whether the card was swiped at a terminal or was a non-swiped transaction.
Valid Values:	The possible values are: <ul style="list-style-type: none"> • "1" for a swiped transaction • "0" for a non-swiped transaction
Maximum Length:	1
Response Version:	2 or higher

avs_result	
Description:	Address Verification System (AVS) response code received on the transaction.
Valid Values:	<p>The valid values are:</p> <ul style="list-style-type: none"> • "A": Street match, zip no match • "N": No match • "S": AVS not supported for this card type • "U": AVS not available for this card type • "W": Zip match 9, street match • "X": Zip match 9, street match • "Y": Zip match 5, street match • "Z": Zip match 5, street no match • "E": Not eligible • "R": System unavailable • "_": Not supported for this network or transaction type <p>There are some international extensions. The following are the valid values for these international extensions:</p> <ul style="list-style-type: none"> • "B": Street match, Zip not verified • "C": Street and Zip not verified • "D": Street and Zip match • "U": Zip match 9, street no match • "M": Street and Zip match • "G": Issuer does not support AVS • "I": Not verified • "P": Street no match, Zip match
Maximum Length:	1
Response Version:	2 or higher

cvv_result	
Description:	Card Verification Value 2 response code. After the payer enters the CVV2 value, it returns the validation result.

cvv_result	
Valid Values:	<p>The valid values are:</p> <ul style="list-style-type: none"> • “_” = Unsupported for network or transaction type • “M” = CVV2 Match • “N” = CVV2 did not match • “P” = CVV2 was not processed • “S” = CVV2 exists but was not input • “U” = Card issuer does not provide CVV2 service • “X” = No response from association • “Y” = CVV2 Match (Amex only when processed through Payroc)
Maximum Length:	1
Response Version:	2 or higher

cvv2_status	
Description:	Flag that checks whether the cvv2 value was provided in the request.
Valid Values:	<p>The possible values are:</p> <ul style="list-style-type: none"> • 1: If a CVV2 value was supplied on the transaction • 0: If a CVV2 value was not supplied on the transaction
Maximum Length:	1
Response Version:	9 or higher

acct_update_id	
Description:	ID of update record used on transaction. Available only for merchants using the Card Account Updater service.
Maximum Length:	12
Response Version:	6 or higher

ACH Payment Information

This section contains the ACH Card Payment information fields related to gateway account.

ach_check_num	
Description:	Check number of a paper check. It is used when paper checks are converted to ACH transfers.
Maximum Length:	15
Response Version:	13 or higher

doc_type	
Description:	ACH Service Entry Class code for the current transaction. See NACHA guidelines for specific requirements related to the usage of each type.
Valid Values:	<p>The valid values are:</p> <ul style="list-style-type: none"> • PPD: Prearranged Payment and Deposit • CCD: Corporate Credit or Debit Entry • WEB: Internet Initiated/Mobile Entry • TEL: Telephone Initiated Entry • CTX: Corporate Trade Exchange Entry • ARC: Account Receivable Entry • POP: Point of Purchase Entry • POS: Point of Sale Entry • BOC: Back Office Conversion Entry
Maximum Length:	3

ach_description	
Description:	Alphanumeric field to identify the type of ACH transaction being performed.
Maximum Length:	10
Response Version:	12 or higher

ach_payout	
Description:	Transaction ID for a payout transaction.
Maximum Length:	12
Response Version:	14 or higher

ach_reject	
Description:	Transaction ID of the corresponding void transaction if a reject notification is received from the bank.
Maximum Length:	12
Response Version:	14 or higher

ach_noc_id	
Description:	Notification of change ID when a transaction is processed using the corrected details received in the ACH NOC file. If ACH_NOC_ID field is blank, then no notification of change information was used to process the transaction.
Maximum Length:	12
Response Version:	14 or higher

ach_trace_number	
Description:	<p>Unique 15-digit trace control number assigned to a transaction whenever it is added to the NACHA settlement file. Originators require this to identify the individual entries.</p> <ul style="list-style-type: none"> • 0-7: The first eight digits of the merchant's routing number that is stored in Immediate Origin on the processor. • 8-14: The remaining seven digits are sequentially numbered from "1" to "9999999" across multiple files on multiple days. The sequential number starts again at "1" once it reaches its maximum limit of "9999999."
Maximum Length:	15
Response Version:	14 or higher

ach_same_day_funding	
Description:	Flag value that indicates if a transaction is funded the same-day.
Valid Values:	<p>The possible values are:</p> <ul style="list-style-type: none"> • "0" or "NULL": The transaction is not funded the same-day • "1": The transaction is funded the same-day
Maximum Length:	1
Response Version:	15 or higher

validation_result	
Description:	Status value that includes bank account validation results from the ACH Account Validation service.
Valid Value:	<p>The valid values are:</p> <ul style="list-style-type: none"> • '15': Known bad bank account. The transaction is immediately declined • '20': Unknown bank account but with a valid format • '25': Unknown bank account • '35': Bank account found but pending transaction settlement (within 5 days) • '45': Known good bank account • 'B': Account validation bypassed • 'R': Bank account validation had failed previously • 'E': Error, bank account validation failed • Null: Account validation not performed
Maximum Length:	2
Response Version:	14 or higher

Customer Information

This section contains the Customer information fields related to gateway account.

name1	
Description:	First name of the customer.
Maximum Length:	32
Response Version:	1 or higher

name2	
Description:	Last name or surname of the customer.
Maximum Length:	32
Response Version:	1 or higher

fancy_name	
Description:	First name and Last name of the customer combined into a single field.
Response Version:	9 or higher

company_name	
Description:	Name of the company on the check or the credit card.
Maximum Length:	64
Response Version:	1 or higher

addr1	
Description:	Street address of the customer.
Maximum Length:	64
Response Version:	1 or higher

addr2	
Description:	Second address of the customer.
Maximum Length:	64
Response Version:	1 or higher

city	
Description:	City name in which the customer resides.
Maximum Length:	32
Response Version:	1 or higher

state	
Description:	State or province in which the customer resides.
Maximum Length:	16
Response Version:	1 or higher

zip	
Description:	Zip or postal code where the customer resides.
Maximum Length:	16
Response Version:	1 or higher

country	
Description:	Name of the country where customer resides.
Response Version:	9 or higher

phone	
Description:	Registered phone number of the customer.
Maximum Length:	16
Response Version:	1 or higher

email	
Description:	Email address of the customer.
Maximum Length:	64
Response Version:	1 or higher

remote_ip	
Description:	Remote IP address captured in the transaction request or the customer's IP address when a POST request is sent through the customer's web browser.
Maximum Length:	15
Response Version:	4 or higher

Additional Transaction Information

This section contains the Additional Transaction information fields related to gateway account.

order_id	
Description:	Merchant-supplied or system supplied order ID.
Maximum Length:	128
Response Version:	1 or higher

invoice_id	
Description:	Merchant-supplied or system supplied invoice ID.
Maximum Length:	64
Response Version:	1 or higher

custom_id	
Description:	Merchant-supplied value for custom ID.
Maximum Length:	16
Response Version:	1 or higher

custom_id2	
Description:	Merchant-supplied value for custom ID 2.
Maximum Length:	64

memo	
Description:	Comment associated with the current transaction.
Maximum Length:	4096
Response Version:	1 or higher

merchdata	
Description:	Additional merchant defined fields containing the merchant supplied data.
Maximum Length:	4096
Response Version:	2 or higher

level_3_data	
Description:	<p>Order and item details related to the card transaction.</p> <ul style="list-style-type: none"> • All the field values starting with "LV2" contain Level 3 order details. For example, shipping amount, discount amount, tax rate and so on. • All the field values starting with "LV3" contain Level 3 item details. For example, item stockkeeping unit, item descriptor, commodity code and so on.
Maximum Length:	4096
Response Version:	3 or higher

level_2_data	
Description:	Purchase identification number along with the tax applied on the transaction.
Maximum Length:	4096
Response Version:	5 or higher

vehicle_rental_data	
Description:	All vehicle rental fields combined into a single field. For example, the value contains vehicle type, vehicle rental agreement number, rent amount, vehicle pick-up and drop-off details and so on.
Response Version:	7 or higher

lodging_data	
Description:	All lodging fields combined into a single field. For example, the value contains lodge folio number, country, extra charges related to Laundry, restaurant, minibar and so on.
Response Version:	7 or higher

Appendix I - Tamper Proof Seals

For a secure transaction, merchants send TAMPER_PROOF_SEAL value in the API request to BluePay. The TAMPER_PROOF_SEAL is used to both authenticate the request and prevent changes in request data. BluePay uses cryptographic hash or “digest” function to calculate the TAMPER_PROOF_SEAL value.

To calculate the hash value, merchants can use any standard hash encoder. Make sure the hash results are in hexadecimal format.

TPS Hash Types

TPS hash type can be any of the following algorithms in hexadecimal form.

Hash Type	Description	# of Hexadecimal Characters in Result
SHA256	Use sha256sum or a similar program to calculate a 256-bit hash, then convert it into hexadecimal form	64
SHA512	Use sha512sum or a similar program to calculate a 512-bit hash, then convert it into hexadecimal form	128
HMAC_SHA256	Use any standard program to calculate a 256-bit hash, then convert it into hexadecimal form	64
HMAC_SHA512	Use any standard program to calculate a 512-bit hash, then convert it into hexadecimal form	128

Calculating the Tamper Proof Seal

STEP 1: Build the pre-hash string

To build pre-hash, concatenate field values in the same order that they are listed in TPS_DEF. If there is no TPS_DEF value in the API request, then use "ACCOUNT_ID REPORT_START_DATE REPORT_END_DATE" as the TPS_DEF value. Use "" (empty string without space) for any fields that are empty or unsent.

Example:

If TPS_DEF="ACCOUNT_ID REPORT_START_DATE REPORT_END_DATE", then TPS_PRE_HASH = ACCOUNT_ID + REPORT_START_DATE + REPORT_END_DATE, where field names represent the values of the respective fields and '+' represents string concatenation.

STEP 2: Perform the Hash

TAMPER_PROOF_SEAL = HASH(Account Secret Key, TPS_PRE_HASH) where HASH is a function that performs the desired hash type.

- If TPS_HASH_VALUE is "" (empty string) or not sent, then the hash function is determined by the "Hash Type in APIs" value on the Account Admin page of the BluePay website.

Example:

Assume the following account information for merchant 'A'

Parameter	Values
Account Secret Key	= "abcdabcdabcdabcd"
Account ID	= "123412341234"
Hash Type in APIs (DEFAULT_HASH_TYPE)	= "HMAC_SHA512"

- If merchant A sets TPS_DEF to "ACCOUNT_ID MODE REPORT_START_DATE REPORT_END_DATE EXCLUDE_ERRORS" and wants to generate transaction report that excludes transaction errors, then the request includes the following parameters.

Parameter	Values
TPS_DEF	= "ACCOUNT_ID MODE REPORT_START_DATE REPORT_END_DATE EXCLUDE_ERRORS"
ACCOUNT_ID	= "123412341234"
EXCLUDE_ERRORS	= "1"
REPORT_START_DATE	= "2021-02-28"
REPORT_END_DATE	= "2021-03-01"
TPS_HASH_TYPE	= ?
TAMPER_PROOF_SEAL	=?

To calculate the TAMPER_PROOF_SEAL, merchant 'A' can perform the following steps

STEP 1:

Concatenate the values in the TPS_DEF to create a pre-hash string.

TPS_PRE_HASH	<pre>= ACCOUNT_ID + EXCLUDE_ERRORS + REPORT_START_DATE + REPORT_ END_DATE + LIMIT_ONE = "123412341234" + "" + "2021-02-28" + "2021-03-01" + "1" = "1234123412342018-02-282021-03-011"</pre>
--------------	---

STEP 2:

Calculate the TPS value in hexadecimal format using the applicable hash type.

TAMPER_PROOF_SEAL	<pre>= HMAC_SHA512 (Account Secret Key, TPS_PRE_HASH) in hex format = HMAC_SHA512("abcdabcdabcdabcd", "1234123412342021-02- 282021-03-011") ="ed0ccd231939d461cb205e7283a0bba09201d20 b516b733f18b578b4cfe0b151daba5884b879442a153b d43814efae1805191eb01e8aee913810aa1204cdae07"</pre>
-------------------	--



To calculate the TPS and retrieve transaction report, you can use sample [BluePay code](#).

Appendix II - Quick Response Field Reference

The following table summarizes the response fields, expected length and minimum response version.

Field Name	Response Version	Maximum Length
id	1	12
payment_type	1	8
trans_type	1	8
amount	1	9
card_type	1	4
payment_account	1	32
order_id	1	128
invoice_id	1	64
custom_id	1	16
custom_id2	1	64
master_id	1	12
status	1	1
f_void	1	1
message	1	64
origin	1	16
issue_date	1	19
settle_date	1	19
rebilling_id	1	12
settlement_id	1	12
card_expire	1	4
bank_name	1	64
addr1	1	64
addr2	1	64
city	1	32
state	1	16

Field Name	Response Version	Maximum Length
zip	1	16
memo	1	4096
phone	1	16
email	1	64
auth_code	1	8
name1	1	32
name2	1	32
company_name	1	64
backend_id	1	2048
f_captured	1	1
avs_result	2	1
cvv_result	2	1
merchdata	2	4096
card_present	2	1
level_3_data	3	
remote_ip	4	
connected_ip	4	
level_2_data	5	
acct_update_id	6	12
vehicle_rental_data	7	
lodging_data	7	
f_refunded	8	1
processor_id	8	12
processor_type	17	8
fancy_name	9	
country	9	
owner_id	9	12
mode	9	4

Field Name	Response Version	Maximum Length
f_rebill_master	9	1
f_will_capture	9	1
f_corporate	9	1
cvv2_status	9	1
account_name	9	
update_id	9	12
f_unheld	9	1
unhold_id	9	12
amount_tip	10	9
f_transarmor	11	1
account_id ¹	1	12
platform_merchant_id	18	20
ach_check_num	13	15
ach_reject	12	12
ach_payout	12	12
ach_noc_id	14	12
validation_result	14	2
ach_same_day_funding	15	1



¹ This field displays only when [QUERY_BY_HIERARCHY](#) is set as "1." and it always displays as the last column regardless of [RESPONSEVERSION](#).

Revision History

Version	Revision Date	Reason for Change
1.0	October 2024	Added the PLATFORM_MERCHANT_ID/platform_merchant_id in the Input Fields, Response Fields, Quick Response Field Reference and Error Responses' Message.
1.1	February 2025	Updated the document layout and format.