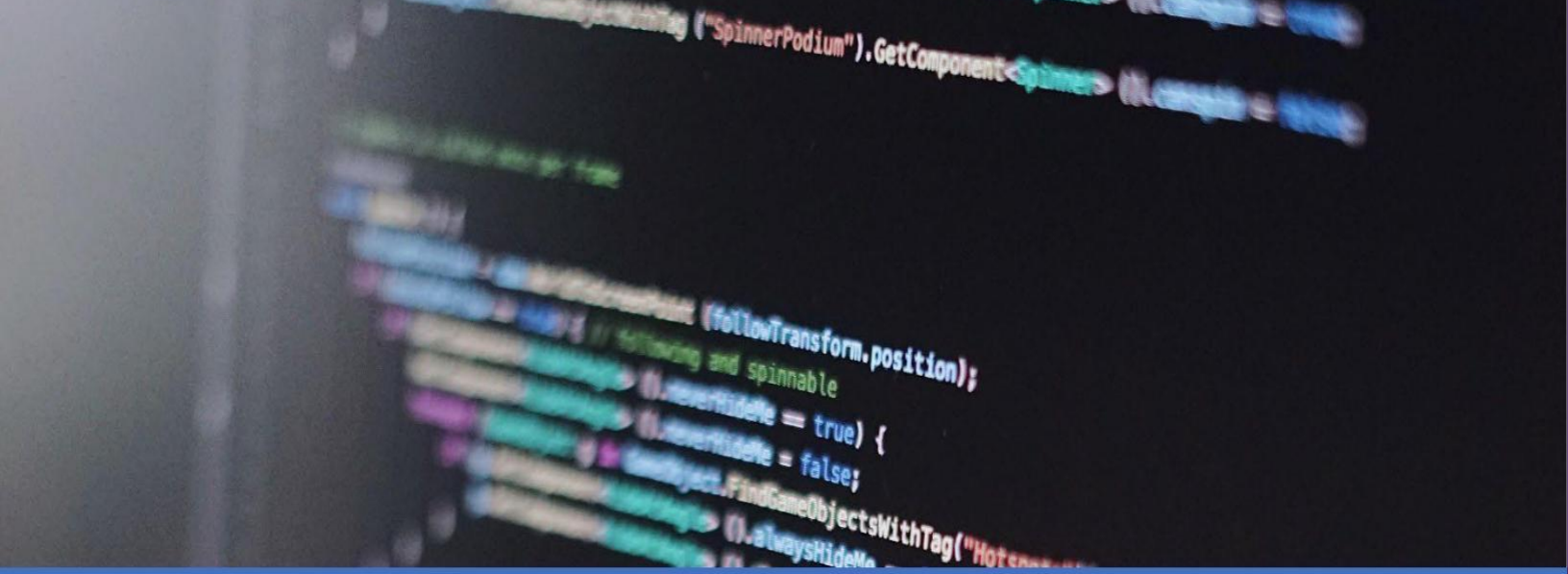
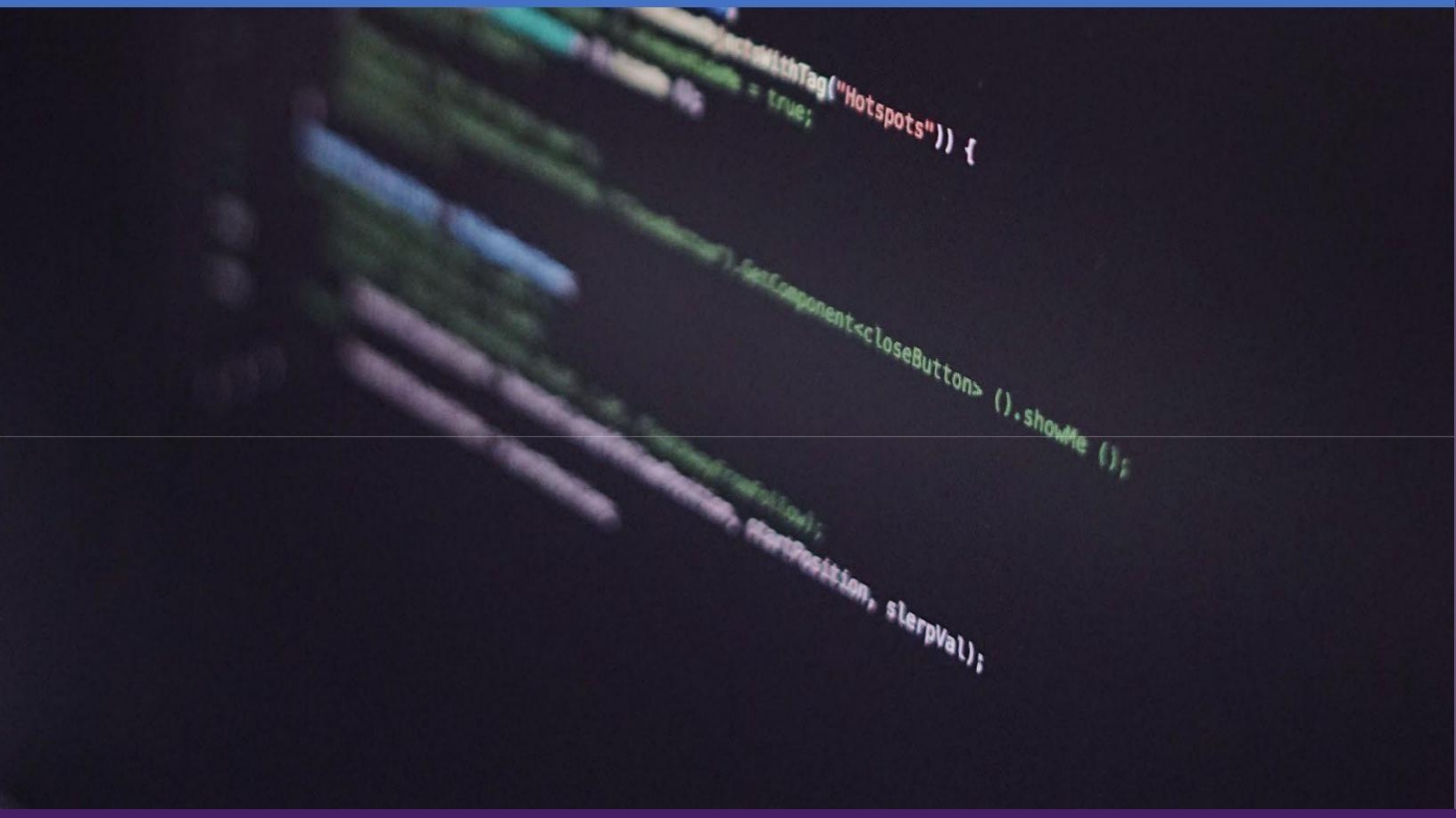


ADVANCED GATEWAY INTERFACE
Integration Guide v3.32

Updated on 02/18/2026



Revision History

Document Version	Date	Changes
3.32	02/18/2026	• Added a parameter to the Transaction Message Template: pg_company_entry_description • Added the Decline codes: U77 & U79
3.31	04/28/2025	Added a parameter to the Response Message Template: pg_avs_code
3.30	12/19/2022	New response codes on appendix A
3.29	12/14/2022	Updates on appendix C
3.28	11/10/2022	Added appendix C
3.27	10/12/2022	Updated U90, U91to P90, P91
3.26	09/22/202	Added/Updated the Transaction Message Template table and the Transaction Type Codes table.
3.25	08/22/2022	Added U32-U35 and U57-U59 codes to Transaction Response Codes
3.24	06/30/2021	Added the U91 and U92 response codes.
3.23	07/16/2020	Added the following parameters: • ecom_payment_card_present • pg_preauth_transaction_id
3.22	02/07/2020	Added the U78 – Disallowed ACH SEC Code to the response code table
3.21	11/18/2019	Updated the description of the pg_cc_enc_emv_data parameter.
3.20	10/29/2019	Changed the Type value for the ecom_payment_card_number parameter.
3.19	10/24/2019	Added pg_cc_enc_emv_data to Message Template and pg_emv_receipt_data to the Response Message to support EMV receipts. Removed Confidential label in footer.
3.18	10/14/2019	Added new COF fields to the AGI Message and Response Templates
3.17	10/03/2019	Made the pg_entry_class_code parameter mandatory.
3.16	08/05/2019	Added the DSI delivery method description back in
3.15	01/15/2019	Added the eDynamo to the list of supported devices for the pg_cc_enc_decryptor parameter.
3.14	04/12/2018	Removed the U01 Transaction Response code as this code no longer exists.

2026 CSG Systems International and/or its affiliates (“CSG”)

Document Version	Date	Changes
3.13	08/31/2017	• Re-added pg_onetime_token parameters to both the Credit Card and EFT Transaction section of the Message Template. • Deleted an inaccurate note from the Message Template regarding the changes from version 3.03.
3.12	10/01/2016	Updated the character limits of the merchant-defined fields (i.e., pg_merchant_data_1-9). Added the following token fields: • pg_customer_token (string tokens) • pg_client_id (integer tokens) • pg_payment_token (string tokens) • pg_payment_method_id (integer tokens)
3.11	02/18/2016	Updated the character limits of the merchant-defined fields (i.e., pg_merchant_data_1-9).
3.10	09/21/2015	Deleted DSI integration method and added the Transaction POST SOAP Web Service.
3.09	07/02/2015	Added note about ecom_consumerorderid field.
3.08	05/19/2015	Deleted decommissioned 3DS fields.
3.07	03/30/2015	Deleted pg_onetime_token from EFT Transaction section of the Message Template.
3.06	01/13/2015	Added the following to the Forte Verify Response Code table: P16 & P72
3.05	12/29/2014	Updated description of Magtek IPAD device #30050203
3.04	11/19/2014	Removed references to the Windows COM Object integration method
3.03	10/13/2014	Branding update
3.02	10/07/2008	Formatting updates
3.01	06/19/2008	Updated Glossary and Index
3.0	06/17/2008	Added and updated the “Best Practices” section
2.3	05/02/2007	Added links to the Table of Contents
2.2	06/22/2006	Added more examples of how to format recurring messages.
2.1	11/04/2005	• Added certification guidance. • Updated the “Setting Up a Live Account” section
2.0	08/19/2005	• Added message and template examples. • Added maintenance recommendations and best practices advice
1.0	11/15/2003	Initial

2026 CSG Systems International and/or its affiliates (“CSG”)

© 2026 CSG Systems International, Inc. and/or its affiliates (“CSG”)

All rights reserved. The information contained in this document is subject to change without notice. CSG makes no warranty of any kind with regard to this material, including but not limited to the documentation, function, and performance of these programs and their suitability for any purpose. CSG shall not be liable for any errors contained herein for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, including trade secrets, which is protected by copyright. All rights are reserved. No part of this document may be reproduced or translated into another document in any language without prior consent of CSG Systems International, Inc., 500 W. Bethany Dr., Suite 200, Allen, TX 75013.

Table of Contents

Overview **8**
Purpose 8
Audience 8
Assistance 8
Integration Overview **9**
Defining a Delivery Method 9
Direct Socket Interface Method 9
Raw HTTP Post 10
SOAP Web Service POST 10
Understanding the Message Template 10
Formatting 10
Codes for Field Types 11
Codes for Field Requirements 11
Transaction Message Template 12
Working with Recurring Transactions **17**
Use Cases 17
Requirements for Recurring Transactions 17
Example 1: Simple Monthly Payments 17
Example 2: Different Recurring Amount and Deferred Recurring Start Date 17
Understanding the Response Message Template 17
Working with Convineince Fees **22**
Convenience Fee Request Fields 22
Convenience Fee Response Fields 22
Adding Line Items **23**
Line Item Fields 23
Line Item Syntax 23
Using Transaction Type Codes in Messages **24**
Transaction Type Codes 24
Setting Up Credit Card Messages **27**
Using Templates 27
Understanding Fields 27
Understanding Settlement 27
Understanding Credit Card Transaction Qualification 27
Verifying Your Transactions 28
Setting Up EFT Messages **29**
Using Templates 29
Understanding Fields 29

2026 CSG Systems International and/or its affiliates (“CSG”)

Understanding Settlement 29
Using Recurring Transaction Admin Messages **30**
Reviewing the Basics 30
Varying the Payment Amount 30
Varying the Date of Payments 31
Creating a Recurring Transaction without a Payment on the Sale Date 31
Method 1: Do not submit the transaction until you want the payments to begin. 31
Method 2: Submit a small payment on the day of the transaction (e.g., a dollar or more) and then set up the remainder of the payments at the corrected amount. 31
Method 3: Set up and run the recurring transaction, then void the original transaction, resulting in recurring payments but no payment on the date of sale. 32
Understanding Response Messages **33**
Testing **34**
Preparing for Testing 34
Ports and URLs 34
Differences Between Test and Live Servers 34
Going Live **35**
Best Practices **36**
Tools Available to Help You 36
Central Point of Contact 36
Obtaining Help from Forte 36
Managing Reconciliation Process 36
Maintaining Documentation 37
Appendix A: Response Codes **39**
Approved and Declined Responses 39
Formatting Error Responses 44
Fatal Error Responses 44
Appendix B: Forte Verify **45**
Verifying Accounts 45
Using Forte Verify 45
Response Values 45
Approval and Forte Verify 46
Authorization and Forte Verify 46
Appendix C: Authenticate: **47**
Ownership Verification 47
Using CSG Forte Authenticate: 47
Response Fields: 47
Response Values: 48
Appendix D: AVS and Other Verification Systems **50**

2026 CSG Systems International and/or its affiliates (“CSG”)

Anonymous Email Check (Position 5) 51
Implicit AVS Checks 51
Appendix E: Example Messages **52**
Credit Card Sale Transaction 52
Credit Card Capture Transaction 52
Credit Card Authorize Only Transaction 52
Credit Card Force Transaction 53
Credit Card Recurring Sale (Initial Charge + 11 Equal Monthly Charges) 53
EFT Sale Transaction 54
EFT Verify Only Transaction 54
EFT Void Transaction 54
Recurring Admin Delete Transaction 54
EFT Sale Transaction Response (with Forte Verify) 54
Glossary **55**
ACH 55
Approval 55
Authorization 55
Authorization Code 55
Auth Only 55
Capture 55
DSI 55
EFT 56
Merchant ID 56
Pre Auth 56
Pre-Notification 56
Procurement Card 56
RAW 56
Reversal 56
Settlement 56
SIC 56
SSL 57
Travel and Entertainment Card 57
Void 57

2026 CSG Systems International and/or its affiliates (“CSG”)

Overview

The Forte Payment Systems platform

1. Captures purchase information via swipe or key entry
2. Processes credit card, EFT, and recurring transactions
3. Automatically responds to your point-of-sale machine approving or denying the transaction
4. Uploads completed transaction information to Forte's Virtual Terminal application (www.paymentsgateway.net/vt3/login.aspx)

Purpose

This guide provides detailed instructions for integrating your point-of-sale system with the Forte platform.

Audience

This guide is intended for technical team members, such as developers, who have experience with the following:

- Basic programming skills
- Basic integration skills and formats
- Your in-house swipe cards system's formats and protocols
- SSL, SOAP, or RAW HTTP Data methods of data transmission

Assistance

For Help	Call	At
During Integration	Forte Technical Support	888-235-4635 option 3
After Integration	Forte Customer Support	800-337-3060 option 1

Forte recommends you assign a project manager to your integration project to manage the necessary setup tasks and connectivity testing. This person should be able to

- *create a comprehensive list of tasks to be completed*
- *create and obtain a list of resources for the dates and durations of the project*
- *manage team members to ensure tasks are completed on time and on budget*
- *be available full-time during testing and go-live phases to ensure all testing is complete*
  - *all staff members are trained on the new system*

2026 CSG Systems International and/or its affiliates ("CSG")

Integration Overview

Forte AGI integrations occur in four steps.

Step	Name	Description
1	Define Delivery Method	Decide which delivery method is more compatible with your current setup: • Direct Socket Interface • Raw HTTP POST • Transaction SOAP POST
2	Compose the Message	Begin creating messages using message type and associated data fields.
3	Test	To ensure a successful integration, thoroughly test the messages you have crated with the options and methods available on the test server.
4	Go-Live	Move all data from the test server to the live server.

Defining a Delivery Method

Use the following chart to determine the best delivery method for your setup.

Method	Description
Direct Socket Interface (DSI)	The Forte platform's native method using a Secure Sockets Layer (SSL) connection.
Raw HTTP Post	A method that uses the HTTP POST protocol to securely deliver messages. This method should only be used if you: • cannot do SSL operations • do not run on a Windows platform
Soap Web Services POST	Use this method for creating payment transactions using the Simple Object Access Protocol (SOAP) web service.

Forte recommends the Direct Socket Interface Method for the most reliable message delivery.

Direct Socket Interface Method

The Direct Socket Interface (DSI) is the native method of the Forte platform and uses a Secure Sockets Layer (SSL) protocol. Authorization request messages are written to an SSL connection and response messages are subsequently read from an SSL connection.
Forte recommends this delivery method because messages are transmitted directly to the transaction processors in the following sequence of steps:

Step	Description
1	Secure socket connects.
2	Transaction message text is read from socket.
3	Response Message text is read from socket.
4	Secure socket is closed.

When sending messages via DSI, the newline (hard return) character must be used as the end - of-line character. Additionally, test and live messages will be sent to different ports. You can implement the DSI method using your own custom server-side software or CGI scripts using any programming language that supports secure sockets.

NOTE: Be sure the appropriate parts are allowed through your firewall.

2026 CSG Systems International and/or its affiliates ("CSG")

Raw HTTP Post

The RAW HTTP POST protocol is intended for

- non-Windows™ merchants
- merchants unable to perform SSL operations
- merchants with access to HTTPS routines

All transactions are routed through the Forte web server in the following sequence of steps:

Step	Description
1	URL encodes the field values (to escape special characters).
2	Concatenate message into an ampersand delimited string.
3	Set the message to be passed as the “content” resource.
4	Perform the POST (URL provided to approved merchants).
5	Forte web server returns newline delimited response message (not HTML).

NOTE: This method sends the POST messages from the merchant’s server and not from the customer’s browser.

SOAP Web Service POST

The SOAP web service supports two Operations:

- **ExecuteSocketDelimitedQuery**: Accepts “strParameters” and “strDelimiter”parameters
- **ExecuteSocketQuery**: Accepts Name Value Pairs

	If you cannot use one of the two delivery methods described above, contact Forte Technical Support to discuss other integration options.

Understanding the Message Template

The following sections describe how to format, create, and process messages.
Creating acceptable messages requires a correct combination of formatting and content fields. These messages should be tested by you and certified by Forte before they can be moved to a production server.

	As you create messages, Forte recommends you document the purpose, follow-up procedures, and content approvals associated with each message. This documentation will make future maintenance easier and help with employee training.

Formatting

Forte platform messages are comprised of name/value fields pairs in the `name=number` format (e.g., a merchant ID would look like `pg_merchant_id=1000`).
Messaging fields

- are always ASCII text (i.e., no binary data)
- can be placed in any order
- must be separated by a newline character when using the DSI delivery method or an ampersand character when using other delivery methods

2026 CSG Systems International and/or its affiliates (“CSG”)

Place an `endofdata` tag at the end of the message immediately followed by a newline character for the DSI delivery method. Messages for other delivery methods should use the appropriate delimiting character after the tag.

The following is an example message:

```
pg_merchant_id=1000 pg_password=abc123
pg_transaction_type=20
pg_total_amount=1.00
ecom_billto_postal_name_first=John
ecom_billto_postal_name_last=Smith
ecom_payment_check_account_type=S
ecom_payment_check_account=012345
ecom_payment_check_trn=123456789
pg_merchant_data_1=just a test endofdata
```

Codes for Field Types

The following table lists the type codes for the fields described in this chapter (in the Transaction Message Template section and the Credit Card and EFT Transaction sections).

Type	Description	Characters Allowed	Case Sensitive ?
M	Money	0-9 (and an optional period)	—
N	Numeric	0-9 (no period)	—
A	Alphanumeric	Any printable ASCII	Yes
L	List-Based Value	Value must be in the specified list	No
D	Date	Format: DD/MM/YYYY	—
T	True / False	“True” or “False” only	No

NOTE: List-Based Values refer to an additional table that lists acceptable values. The value used in the message must be one included in the value list. **True/False** fields are considered false if there is no indicator present in the **Type** field of the message.

Codes for Field Requirements

The following table lists the requirement codes for the fields described in this chapter (in the Transaction Message Template section and the Credit Card and EFT Transaction sections).

Code	Requirement	Description
M	Mandatory	Must appear when the table’s fields are used
O	Optional	May appear when table’s field are used
C	Conditional	See description for exact requirements
R	Response Only	Only appears in response message

2026 CSG Systems International and/or its affiliates (“CSG”)

Transaction Message Template

The following groups of fields make up the template for the core portion of the transaction message.

Group	Field Name	Description	Type	Req
Header	pg_merchant_id	The merchant's six-digit code	N9	M
	pg_password	The merchant's processing password	A20	M
	pg_transaction_type	Indicates the transaction type	L	M
	pg_transaction_subtype	Indicates the sub-transaction type. Note: The only value that is valid is "authenticate" and it applies only when pg_transaction_type = 26.	L	O
	pg_merchant_data_1-9	Up to nine field returned with the response fields	A255	O
Customer / Order Info	pg_total_amount	Amount to be charged/credited to the customer	M	M
	pg_sales_tax_amount	Sales tax amount	M	C(PC)
	pg_consumer_id	ID assigned by the merchant and returned with the response	A15	O
	ecom_consumerorderid[1]	ID assigned by the merchant and returned with the response	A36	O
	ecom_walletid	ID assigned by the merchant and returned with the response	A15	O
	pg_customer_token	Unique string ID that references a customer's stored information	A50	O
	pg_client_id	Unique integer ID that references a customer's stored information. Returned with response	N50	O
	pg_billto_postal_name_company	Company name	A20	O
	ecom_billto_postal_name_first	Customer's first name	A25	M
	ecom_billto_postal_name_last	Customer's last name	A25	M
	ecom_billto_postal_street_line1	Customer's street address	A35	C(AVS)
	ecom_billto_postal_street_line2	Customer's street address	A35	O
	ecom_billto_postal_city	Customer's city	A25	O
	ecom_billto_postal_stateprov	Customer's state (abbreviated)	A10	C(AVS)
	ecom_billto_postal_postalcode	Customer's ZIP code	A10	C(AVS)
	ecom_billto_postal_countrycode	Customer's country	A2	O
	ecom_billto_telecom_phone_number	Customer's phone number	A15	C(AVS)
	ecom_billto_online_email	Customer's email address	A40	C(AVS)

2026 CSG Systems International and/or its affiliates ("CSG")

<table>
<tr><th>Group</th><th>Field Name</th><th>Description</th><th>Type</th><th>Req</th></tr>
<tr><td></td><td>pg_billto_ssn</td><td>Customer's Social Security Number</td><td>A11</td><td>O</td></tr>
<tr><td></td><td>pg_billto_dl_number</td><td>Customer's Driver's License number</td><td>A20</td><td>O</td></tr>
<tr><td></td><td>pg_billto_dl_state</td><td>Customer's Driver's License state</td><td>A2</td><td>O</td></tr>
<tr><td></td><td>pg_billto_date_of_birth</td><td>Customer's date of birth in MM/DD/YYYY format</td><td>D</td><td>O</td></tr>
<tr><td></td><td>pg_entered_by</td><td>Name or ID of the person entering the data; appears in the Virtual Terminal transaction display window</td><td>A20</td><td>O</td></tr>
<tr><td>Recurring</td><td>pg_schedule_quantity</td><td>Specifies the number of recurring transactions</td><td>N9</td><td>C(R)</td></tr>
<tr><td></td><td>pg_schedule_frequency</td><td>Specifies the frequency of the recurring transactions.
Use the following values:<table><tr><th>Value</th><th>Frequency</th><th>Period</th></tr><tr><td>10</td><td>Weekly</td><td>Every 7 days</td></tr><tr><td>15</td><td>Bi-Weekly</td><td>Every 14 days</td></tr><tr><td>20</td><td>Monthly</td><td>Same day every month</td></tr><tr><td>25</td><td>Bi-Monthly</td><td>Every 2 months</td></tr><tr><td>30</td><td>Quaterly</td><td>Every 3 months</td></tr><tr><td>35</td><td>Semi-Annually</td><td>Twice a year</td></tr><tr><td>40</td><td>Yearly</td><td>Once a year</td></tr></table></td><td>L</td><td>C(R)</td></tr>
<tr><td></td><td>pg_schedule_recurring_amount</td><td>Specifies the amount of the recurring transaction if different from the initial transaction.</td><td>M</td><td>C(R)</td></tr>
<tr><td></td><td>pg_schedule_start_date</td><td>Specifies the start date of the next recurring transaction in the MM/DD/YYYY format and may only be used with the pg_schedule_recurring_amount field</td><td>D</td><td>C(R)</td></tr>
<tr><td>Misc.</td><td>pg_customer_ip_address</td><td>Customer's originating IP address (used for fraud prevention)</td><td>A80</td><td>O</td></tr>
<tr><td></td><td>pg_merchant_recurring</td><td>When used in conjunction with CC transactions, a recurring indicator will be included with the authorization message to the issuer, which may affect qualification</td><td>T</td><td>O</td></tr>
<tr><td></td><td>pg_software_name</td><td>Name of the software application used to create the transaction</td><td>A20</td><td>O</td></tr>
<tr><td></td><td>pg_software_version</td><td>Version of the software application used to create the transaction</td><td>A20</td><td>O</td></tr>
<tr><td></td><td>pg_avs_method</td><td>Specifies which AVS checks to perform on the transaction (if any); makes some optional fields required.</td><td>N5</td><td>O</td></tr>
<tr><td></td><td>pg_preauth_transaction_id</td><td>Indicates the authorization code for Force transactions. This field only applies to TSYS merchants.</td><td>A15</td><td>O</td></tr>
<tr><td>Credit Card Transaction</td><td>pg_payment_token</td><td>Unique string ID that references a customer's stored payment information. Returned with response.</td><td>A50</td><td>O</td></tr>
</table>

2026 CSG Systems International and/or its affiliates ("CSG")

Group	Field Name	Description	Type	Req
	pg_payment_method_id	Unique integer ID that references a customer's stored payment information. Returned with response	N50	O
	pg_onetime_token	A one-time-use token that references stored payment information.	A50	O
	ecom_payment_card_type	The credit card issuer. Use one of the following values: Type / Issuer VISA / VISA MAST / MasterCard AMER / American Express DISC / Discover DINE / Diner's Club JCB / JCB	L	M
	ecom_payment_card_name	Cardholder name as it appears on the card	A50	M
	ecom_payment_card_number	Card account number Note: Device Primary Account Number for Alternative Method of Payments.	N19	M
	ecom_payment_card_exp_date_month	Numeric month of expiration (e.g., January = 1)	N2	M
	ecom_payment_card_exp_date_year	Four-digit year of expiration	N4	M
	ecom_payment_card_verification	CVV2/verification number	N5	O
	pg_procurement_card	Indicates procurement card transaction, requires pg_sales_tax_amount and pg_customer_acct_code fields	T	O
	pg_customer_acct_code	Accounting information for procurement card transactions	A17	C(PC)
	ecom_payment_card_present	Indicates if a card was present for a manually entered transaction. This field only applies to TSYS merchants.	T	O
	pg_cc_swipe_data	Magstripe data from track one or two	A80	O
	pg_cc_enc_swipe_data	Full set of swipe data received from the encrypting device	A1500	O
	pg_cc_enc_decryptor	The eight-digit device part number in parenthesis below specifying which swipe device was used. Currently, only the following models and part numbers are supported when capturing encrypted card data: • iPad (30050203) • Dynamag (21073062) • iDynamo (21073084) • uDynamo (21073092) • eDynamo (21079802)	L20	O
	pg_cc_enc_emv_data	The encrypted EMV data for encrypted MagTek EMV devices. The format of this field is KSN|ARQC. • KSN is the Key Serial Number and ARQC is the data found at tag DFDF59 after dipping the card while using MagTek's Web API.	A1500	O

2026 CSG Systems International and/or its affiliates ("CSG")

Group	Field Name	Description	Type	Req
	pg_partial_auth_allowed_flag	For merchants approved to process partial authorizations, set this field to override default merchant settings. Supported authorizing vendors: GlobalPayments and FirstData	T	O
	pg_mail_or_phone_order	Indicates mail order or phone order transaction (as opposed to an online transaction)	T	O
	pg_cof_transaction_type	Indicates whether the credential on file (COF) transaction is recurring (0) or customer initiated (1). **NOTE**: If you are performing a zero-dollar authorization and only storing the payment method for future use, then the pg_cof_transaction_type should be 1.	N1	O[2]
	pg_cof_initial_transaction_id	The processor's transaction ID of the first transaction for a stored credential on file.	A20	C[3]
EFT Transaction	pg_payment_token	Unique string ID that references a customer's stored payment information.		
	pg_payment_method_id	Unique integer ID that references a customer's stored payment information.		
	pg_onetime_token	A one-time-use token that references stored payment information.		
	ecom_payment_check_trn	Transit routing number (ABA) for customer's account	N9	M
	ecom_payment_check_account	Customer's account number	N17	M
	ecom_payment_check_account_type	Type of bank account. Use one of the following values: • S= Savings Account • C= Checking Account	L	M
	ecom_payment_check_checkno	Check number for point-of-sale transactions	N10	O
	pg_entry_class_code	The standard entry class code. Use one of the following values: • ARC • CCD • CIE • CTX • POP • POS • PPD • RCK • TEL • WEB **NOTE**: If the entry class code is not specified, the pg_entry_class_code will default to PPD or, if established, the override entry class code value within the Merchant Setup. Specify the proper entry class code for each transaction.	A3	M

2026 CSG Systems International and/or its affiliates ("CSG")

Group	Field Name	Description	Type	Req
		Improper entry class code usage can result in fines for NACHA violations or hurt the merchant's ability to prevent items from being returned (charged back) in customer dispute situations.\		
	pg_company_entry_description	This field is for the Merchants to pass a company entry description for ACH transactions. • Supports up to 10 characters; values longer than 10 characters will be truncated. • Only letters, numbers, and spaces are allowed. • Invalid characters return error code F04 - INVALID FIELD VALUE. • Available for transaction types 20, 21, 23, and 25.	A10	O
Admin Message	pg_merchant_id	The merchant's six-digit ID code.	N8	M
	pg_password	The merchant's processing password	A20	M
	pg_transaction_type	Indicates the transaction type.	L	M
	pg_merchant_data_[1-9]	Nine fields returned with the response fields	A255	O
	pg_original_trace_number	The trace number returned by the original transaction to be affected	A36	M
	pg_original_authorization_code	The authorization code returned with the above trace number (voids and captures only)	A80	$C_{(AC)}$

- *Some credit card authorizers/settlement vendors require the ecom_consumerorderid field to be numeric for qualification. For those vendors, Forte normalizes and randomly assigns an integer value to the field.*
- *Recommended when using stored credentials to meet VISA's credential-on-file mandate. This includes transactions with Forte tokens that don't use Forte schedules and transactions using merchant managed cardholder data.*
- *Required for non-tokenized credential-on-file subsequent transactions.*
  - *(AC)–The pg_original_authorization_code field is only required for credit card and EFT capture and void transactions*
  - *(AVS)–Indicates a field that is required for AVS checks specified in the pg_avs_method field and optional otherwise. (PC)–Indicates a field that is required for procurement card transactions and optional otherwise.*
  - *(R)–Indicates a field that is required for recurring transactions and optional otherwise.*

2026 CSG Systems International and/or its affiliates ("CSG")

Working with Recurring Transactions

The fields listed in the Recurring group of the Transaction Message Template establish recurring transactions by specifying the frequency and quantity of a recurring transaction. These transactions occur until

- the specified quantity is reached (if it is non-zero)
- the transaction is suspended or deleted by the merchant

NOTE: Voided and declined transactions do not count toward the specified quantity.

Use Cases

These fields provide the flexibility to accommodate several use cases. For example, if the customer wanted to specify a set number of recurring transactions after making an initial transaction (such as a down payment), the merchant would specify the `pg_total_amount` field for the initial transaction and use the `pg_scheduled_recurring_amount` field to define the amount for the subsequent recurring transactions (the initial transaction does not count toward the specified quantity).
To define when the first recurring transaction should occur, use the `pg_schedule_start_date` field with the `pg_schedule_recurring_amount` field. If the start date is on or before the day the initial transaction is processed, the next start date will be the following day.

Requirements for Recurring Transactions

Recurring transactions submitted like the use case described above depend upon an approved initial transaction. Forte will not schedule a recurring transaction if the original transaction is declined. Additionally, a merchant cannot use this method to create recurring transactions that do not begin at the time of submission. Setting the initial amount to less than $1 (including $0) results in a decline from most credit card processors/banks.

Example 1: Simple Monthly Payments

If the transaction is approved, the code displayed below will result in eleven more $10 transaction being processed on the same day of the month that the initial transaction was approved.

```
pg_total_amount=10.00
pg_schedule_quantity=12
pg_schedule_frequency=20
```

Example 2: Different Recurring Amount and Deferred Recurring Start Date

The following code displays a recurring transaction with a different initial transaction amount and a specified start date. If the initial $100 transaction is approved, eight more $25 transactions will be processed monthly beginning on 6/1/2005.

```
pg_total_amount=100.00
pg_schedule_quantity=8
pg_schedule_frequency=20
pg_schedule_recurring_amount=25.00
pg_schedule_start_date=06/01/2005
```

Understanding the Response Message Template

The following table lists the fields that may appear in the response message. Some fields are always present, some will be present if they were in the original message, and others will be present based on other criteria including the original message transaction type.

2026 CSG Systems International and/or its affiliates (“CSG”)

The Comments column indicates in what circumstances the fields appear in the message.

Field Name	Type	Description	Comments
pg_merchant_id	N8	The merchant's six-digit ID code	Always present
pg_transaction_type	L	Indicates the transaction type	Always present
pg_merchant_data_[1-9]	A255	Up to nine merchant- defined fields	Echoed if specified
pg_total_amount	M	Amount to be charged/credited to the customer	Echoed if specified
pg_sales_tax_amount	M	Sales tax amount	Echoed if specified
pg_customer_token	A50	Unique string ID that references a customer's stored information	Echoed if specified
pg_client_id	N50	Unique integer ID that references a customer's stored information. Returned with response.	Echoed if specified
pg_consumer_id	A15	ID assigned by the merchant and returned with the response	Echoed if specified
ecom_consumerorderid	A36	ID assigned by the merchant and returned with the response	Echoed if specified
pg_payment_token	A50	Unique string ID that references a customer's stored payment information. Returned with response.	Echoed if specified
pg_payment_method_id	N50	Unique integer ID that references a customer's stored payment information. Returned with response.	Echoed if specified
ecom_walletid	A15	ID assigned by the merchant and returned with the response	Echoed if specified
ecom_billto_postal_name_ first	A25	Customer's First Name	Echoed if specified
ecom_billto_postal_name_ last	A25	Customer's Last Name	Echoed if specified
pg_billto_postal_name_ company	A20	Company name	Echoed if specified
ecom_billto_online_email	A40	Customer's email address	Echoed if specified
pg_emv_receipt_data	A200	The additional fields required in order to print an EMV-compliant receipt. This is a pipe delimited list of key/value pairs that are required to be printed on EMV compliant receipts.	Echoed if specified
pg_response_type	L	Single letter response that indicates the success or failure of a transaction. Use	Always present

2026 CSG Systems International and/or its affiliates ("CSG")

Field Name	Type	Description	Comments
		the following values: • A= Approved • D= Declined • E= Error	
pg_response_code	A3	Three-character code representing the transaction result (see the tables in Appendix A)	Always present
pg_response_description	A80	Text description of the transaction results	Always present
pg_avs_result	N5	Five digits representing the outcome of the requested AVS checks (see Appendix C for detailed information)	Present if AVS method specified
pg_avs_codes	L	Single letter response that indicates the outcome of the requested AVS checks (see Appendix C for detailed information). Use the following values: • X= Match: Street Address and 9-digit Zip Code both match • Y= Match: Street Address and 5-digit Zip Code both match • A= Partial Match: Street Address matches, but both 5-digit and 9-digit Zip Code do not match • W= Partial Match: Street Address does not match, but 9-digit Zip Code matches • Z= Partial Match: Street Address does not match, but 5-digit Zip Code matches • N= No Match: Street Address, 5-digit Zip Code, and 9- digit Zip Code all do not match • U= System Unavailable: Address information unavailable. Forte returns this response if the Street Address is a non-US address, if the AVS service is unavailable, or if the AVS service for a	Always present

2026 CSG Systems International and/or its affiliates (“CSG”)

Field Name	Type	Description	Comments
		particular US bank is not properly functioning. • R= System Unavailable: Forte will retry the AVS check because the issuer's system is unavailable or the request times out. • Invalid: AVS data is invalid • S= Not Supported: The US issuing bank does not support AVS checks.	
pg_trace_number	A36	36-character code uniquely identifying the transaction	Always present
pg_authorization_code	A8	8-character approval code from the vendor providing credit card or EFT authorization	Present if authorization performed
pg_preauth_result	L	Pre-authorization check result (i.e., Forte Verify) using the following values: • POS = Positive • NEG = Negative • UNK = No information available	Present if pre-authorization performed
pg_preauth_description	A80	Text description of the pre-authorization result	Present if pre-authorization performed
pg_preauth_neg_report	A80	Negative database response information (unformatted)	Generally, provides details on the negative pre- authorization decline and contact information for consumer inquiries when it is available
pg_requested_amount	M	The originally requested amount for partially authorized transactions.	The originally requested amount for partially authorized transactions
pg_available_card_balance	M	Field present if partial authorization or balance inquiry was performed and balance was returned by the authorizing vendor.	Present if partial authorization or balance inquiry was performed and balance was returned by the authorizing vendor
pg_cvv2_result	A1	This field is present in Global and Vital responses for credit card transactions with CVV2 information. Single character result code (e.g., Mfor match or Nfor no match). Other responses are possible but may be ignored. NOTE: Transactions declining or being approved on the	Present for credit card transactions with CVV2 information sent to Global-Payments and Vital

2026 CSG Systems International and/or its affiliates ("CSG")

Field Name	Type	Description	Comments
		CVV2 code is at the sole discretion of the card issuer.	
pg_cvv_code	L	Single-letter response that indicates the outcome of a CVV verification for credit card transactions. Use the following values: • M= Match • N= No Match • E= Error (Unrecognized or Unknown Response) • I= Invalid or Null • P = Not Processed • S = Service Not Supported • U = Issuer Unable to Process • X = No Response	Always present for credit card transactions
pg_cof_initial_transaction_id	A20	The processor's transaction ID	This is present only when: • pg_cof_transaction_type is provided, • pg_cof_initial_transaction_id is not provided, • Forte tokens aren't being used, and • Forte schedules aren't being used

2026 CSG Systems International and/or its affiliates ("CSG")

Working with Convineince Fees

Merchant accounts approved to process convenience fee transactions should include additional fields in their transaction requests. Consequently, an additional field is returned in the transaction response.

Convenience Fee Request Fields

The following table displays the existing field (shaded) and the new field merchants can use to capture convenience fees:

Group	Field Name	Description	Type	Req
Convenience Fee	pg_total_amount	The total amount, including the transaction fee to be charged	M	M
	pg_convenience_fee	The amount of the convenience fee	M	M

Forte uses these fields to calculate the original amount (total amount– convenience fee = original amount) and check it against the convenience fee information in the database for the merchant account specified in the pg_merchant_id field. If the convenience fee is incorrect, Forte declines the transaction with the following response:

```
pg_response_code=U28
pre_response_description=CONV FEE INCORRECT
```

Convenience Fee Response Fields

The following field displays in the transaction response after the merchant has specified a convenience fee in the request:

Group	Field Name	Description	Type	Req
Convenience Fee	pg_convenience_fee	The amount of the convenience fee	M	M

2026 CSG Systems International and/or its affiliates (“CSG”)

Adding Line Items

Merchants can include up to 100 line items by passing the line item fields in their transaction message(s).

Line Item Fields

The following table displays the fields for line items in a transaction message. Header and item lines allow for a maximum of 8000 characters.

Group	Field Name	Description	Type	Req
Line Items	`pg_line_item_header`	Description of the data elements contained within each line item. This header will be displayed when viewing transaction details within the Virtual Terminal.	A256	O
	`pg_line_items_(1-100)`	Contents of the line item formatted according to `pg_line_item_header`.	M	M

Line Item Syntax

The example below displays the syntax for line items in a transaction message.

```
pg_line_item_header=col1,col2,col3
pg_line_item_1=value1,value2,value3
pg_line_item_2=value1,value2,value3
pg_line_item_3=value1,value2,value3
```

The example below displays how this syntax looks with data:

```
pg_line_item_header=SKU,Price,Qty
pg_line_item_1=021000021,45.00,2
pg_line_item_2=021000022,36.99,10
pg_line_item_3=021000023,27.50,7
```


2026 CSG Systems International and/or its affiliates (“CSG”)

Using Transaction Type Codes in Messages

Every transaction that Forte processes must be assigned a transaction type via the `pg_transaction_type` field.

This chapter lists these fields.

Transaction Type Codes

The following table displays the fields for line items in a transaction message. Header and item lines allow for a maximum of 8000 characters.

Group	Type	Name	Description	Comments
Credit Card	10	Sale	Customer's card is charged and will be automatically settled at the end of the day	Customer is charged
	11	Auth Only	Customer's card is charged but will not be settled until a `CAPTURE` message is completed.	Authorization only, `CAPTURE` transaction required
	12	Capture	Completes an `AUTH ONLY` transaction. The original charge will be settled at the end of the day.	Completes `AUTH ONLY` transaction
	13	Credit	Customer's card is credited and will be automatically settled at the end of the day.	Customer is credited
	14	Void	If the target transaction has not be settled, it will be voided (and never be settled). Attempts to void a settled transaction will be declined (with an appropriate response code).	Cancel non- settled transactions
	15	Pre-Auth	The customer's card is charged using a merchant-supplied authorization code (received from the card processor directly). This is sometimes referred to as a `FORCE` transaction. Using a merchant-supplied authorization code (received from the card processor directly). This is sometimes referred to as a `FORCE` transaction.	Customer charge approved from other source

2026 CSG Systems International and/or its affiliates ("CSG")

Group	Type	Name	Description	Comments
	18	Balance Inquiry	For merchant accounts approved to process partial authorization transactions, this field requests the available balance from a card. For this transaction type, do not include the `pg_total_amount` field. Supported authorizing vendors: GlobalPayments and FirstData.	Requests the available balance from a card
	20	Sale	Transaction is completed and the funds will be captured at the end of the day.	Customer is charged
EFT	21	Auth Only	Transaction is authorized, but the funds are not captured until a `CAPTURE` message is completed.	Authorization only, `CAPTURE` transaction required
	22	Capture	Completes an `AUTH ONLY` transaction. The funds for the original transaction will be captured at the end of the day.	Completes `AUTH ONLY` transaction
	23	Credit	Transaction is completed and the funds will be transferred at the end of the day.	Customer is credited
	24	Void	If the target transaction has not been settled, it will be voided (and will never be settled). Attempts to void a settled transaction will be declined (with an appropriate response code).	Cancels non- settled transactions
	25	Force	Transaction is completed and the funds will be captured at the end of the day. Verification checks are skipped for this type of transaction. You must contact Forte Customer Service to put an `EFT FORCE` into place	Customer charged (no validation checks)
	26	Verify Only	Transaction is verified but no authorization is obtained, and it cannot be settled. This is for use with Forte Verify. For these transactions, the “Customer/Order Information”fields are all optional except for amount.	Verification only, no customer charge

2026 CSG Systems International and/or its affiliates (“CSG”)

Group	Type	Name	Description	Comments
	26	Authenticate	To verify the ownership of a bank account, it requires the additional field pg_transaction_subtype=authenticate.	
Recurring	40	Suspend	The (active) recurring transaction is put into a suspended state. No more transactions will be generated on its behalf until it is reactivated.	Suspends a recurring transaction
	41	Activate	The (suspended) recurring transaction is returned to an active state. Transactions will again be generated on its behalf.	Reactivates a recurring transaction
	42	Delete	The recurring transaction will be deleted permanently.	Deletes a recurring transaction.

2026 CSG Systems International and/or its affiliates (“CSG”)

Setting Up Credit Card Messages

The following chapter provides notes and helpful hints for setting up credit card messages.

Using Templates

When setting up messages for `SALE`, `AUTH ONLY`, `CREDIT`, and `PRE-AUTH` transaction messages (types `10`, `11`, `13`, and `15`, respectively), use the fields of the Credit Card Transaction group of the Transaction Message Template. When creating `CAPTURE` and `VOID` transaction messages (types `12` and `14`), use the fields of the Administrative Message group of the Transaction Message Template.

Understanding Fields

The AVS field can be used with `SALE` and `AUTH ONLY` transactions (because credits do not require preauthorization, and `PRE-AUTH` transactions have already been authorized). The miscellaneous "PREAUTH" fields are not used in credit card messages.

Recurring fields can be used only for `SALE` and `CREDIT` messages. Procurement card transactions must have the `pg_procurement_card` field set to `TRUE` and require the sales tax and customer account codes.

Magstripe data (track one or two) may be included in the swipe data field. Mail order and phone order transaction must include the `pg_mail_phone_order` field set to `TRUE`.

Understanding Settlement

`SALE`, `CREDIT`, and `FORCE` transactions settle at the end of the day. `AUTH ONLY` transactions settle at the end of the day that their corresponding `CAPTURE` message is approved. Only unsettled transactions may be voided. Voided transactions are never settled.

`CAPTURE` and `VOID` messages require the original authorization code in addition to the original trace number.

Understanding Credit Card Transaction Qualification

"Downgrading" can occur when a portion of information is missing from the credit card authorizing request. This may result in a higher fee for the offending transaction. Downgrading typically (although not always) occurs when a card must be manually keyed into the system and some information required by the credit provider is omitted.

To qualify as swipe transactions, retail transactions typically require information in the swipe data fields. Contact your credit card provider for specific rules. Each credit provider has different rules about what data elements constitute a fully qualified transaction.

Forte is not responsible for transaction downgrading. The merchant is responsible for contacting his/her credit providers, learning which data elements are required, and ensuring his/her messages contain that data.

2026 CSG Systems International and/or its affiliates ("CSG")

Verifying Your Transactions

Forte recommends that immediately after go-live, you contact your credit providers to ensure that the information you are sending them meets their standards for a fully qualified transaction. Contacting them early can help you avoid needless expenses.
Some customers have waited until receiving a statement from their provider,only to discover that they were neglecting to enter a key piece of data, resulting in thousands of downgraded transactions.

The following tips may help you prevent your credit card transactions from being downgraded:

1. Non-swipe transactions should include street address and zip code information so an AVS check can be performed. Forte also recommends keying in the
2. CVV/CVV2/CIV/CID data.
3. Include invoice, ticket, or P.O. numbers in the `ecom_consumerorderid` field.
4. When keying in purchase and/or corporate cards, use the `pg_sales_tax_amount` and `pg_customer_acct_code` fields.

2026 CSG Systems International and/or its affiliates (“CSG”)

Setting Up EFT Messages

The following section provides notes and helpful hints for setting up electronic funds transfer (EFT) messages.

Using Templates

The SALE, AUTH ONLY, CREDIT, and FORCE messages (types 20, 21, 23, and 25, respectively) use the fields of the EFT Transactions group of the Transaction Message Template. The CAPTURE and VOID messages (types 22 and 24) use the fields of the Administrative Message group of the Transaction Message Template.

Understanding Fields

The AVS field can be used with SALE and AUTH ONLY transactions. Only SALE, CREDIT, and FORCE messages can include the recurring fields. The check number field is only used for point-of-sale transactions.

Understanding Settlement

SALE, CREDIT, and FORCE transactions settle at the end of the day. AUTH ONLY transactions settle at the end of the day that their corresponding CAPTURE message is approved. Only unsettled transactions may be voided. Voided transactions are never settled.
CAPTURE and VOID messages require the original authorization code in addition to the original trace number.

2026 CSG Systems International and/or its affiliates (“CSG”)

Using Recurring Transaction Admin Messages

You use recurring transaction admin messages to activate, suspend, and delete existing recurring transactions. These messages use the Admin Message Template of the Transaction Message Template and differ only in their transaction type. Deleted recurring transactions cannot be activated or suspended.
The trace number returned by the original transaction is required by these messages.
Setting up and using recurring transactions can be confusing to some end users because recurring payments can be set up in different ways.
The following sections detail common scenarios using recurring payments.

Reviewing the Basics

Recurring transactions with the three fields listed above have the simplest setup:
The original date of the sale is the same day of the month any future payments will be made.
All payments will be the same amount, which is the amount charged on the day of the sale.

For example, if the recurring transaction included the following information,

```
pg_total_amount=100.00
pg_schedule_frequency=20
pg_schedule_quantity=12
```

then the transaction would include a total of 12 payments (including the initial payment) starting monthly from date of the sale and

`1 x $100 = $100` *//Equals the initial transaction on the submission date*
`11 x $100 = $1100` *//Equals the remaining payments in the recurring schedule*

with a Grand Total = $1200.00 between a total of 12 payments.

Varying the Payment Amount

To create transactions where the amount on the original sale date is different from the amount of subsequent payments, use the `pg_total_amount` field to specify the amount to be processed on the date of sale and the `pg_schedule_recurring_amount` field to specify the amount of recurring payments.
For example, given

```
pg_total_amount=53.2
pg_schedule_quantity=12
pg_schedule_frequency=20
pg_schedule_recurring_amount=100.00
```

The first payment is $53.20. In subsequent months, on the same day of the month as the first payment, $100.00 will be deducted from the customer's account until a total of 13 payments have been deducted (including the first payment).
With these 13 payments, the total amount paid equals:

```
12 x $100 = $1200.00 1 x $53.20 = $53.20
$1200.00 + $53.20 = $1253.20
```


2026 CSG Systems International and/or its affiliates ("CSG")

Varying the Date of Payments

Most customers want their payments to fall on a specific day of the month. Use the `pg_schedule_start_date` field to accomplish this.

To create transaction where the date of the recurring payments is different from that of the original sale date, use the `pg_schedule_start_date` field to specify the date when recurring payments should begin. If the start date is on or before the day the initial transaction is processed, the next start date will be the following day.

For example, given

```
pg_total_amount=53.20
pg_schedule_quantity=12
pg_schedule_frequency=20
pg_schedule_recurring_amount=100.00
```

The second and subsequent payments are deducted on the first day of every month. With these 13 payments, the total amount paid equals:

`12 x $100 = $1200.00`

Deducted on the first of every month `1 x $53.20 = $53.20`

Taken on the date of sale

`$1200.00 + $53.20 = $1253.20`

Creating a Recurring Transaction without a Payment on the Sale Date

You can create recurring transactions without a payment on the date of sale through one of three methods that Forte recommends:

Method 1: Do not submit the transaction until you want the payments to begin.

This manual solution requires that you hold transaction records and submit them on the exact date to be used for all future payments. You would submit the payment on that date, which would then be used for all future subsequent payments. For example, if a customer wanted to purchase a new chair for $1000 and wants to pay for it over a 10-month period beginning on the first of the next month, you would need to hold the sales slip until the first of the month
and then submit the transaction.

Method 2: Submit a small payment on the day of the transaction (e.g., a dollar or more) and then set up the remainder of the payments at the corrected amount.

For example, to set up the purchase of a $1000 chair over 10 months beginning June 1, 2006, use the following code:

```
pg_total_amount=1.00
pg_schedule_quantity=10
pg_schedule_frequency=20
pg_schedule_recurring_amount=99.90
pg_schedule_start_date=6/1/2006
```


2026 CSG Systems International and/or its affiliates (“CSG”)

In this example, the customer pays $1.00 on the purchase date and pays $99.90 per month every month for the next 10 months beginning on June 1, 2006. This method can also be used even if the purchase amount is not evenly divisible by the number of payments.
For example, if the chair including sales tax cost $1003.38, the merchant could charge $3.38 to the customer's card on the day of the sale and then set up the remaining 10 payments of $100 each, as shown below:

```
pg_total_amount=3.38
pg_schedule_quantity=10
pg_schedule_frequency=20 p
g_schedule_recurring_amount=100.00
pg_schedule_start_date=6/1/2006
```

Method 3: Set up and run the recurring transaction, then void the original transaction, resulting in recurring payments but no payment on the date of sale.

To use this method, you would set up the transaction as described in method 2 above. After obtaining confirmation that the transaction is accepted, you must immediately void the transaction. The first payment (e.g., the $1.00 payment) will be authorized but voided, resulting in no actual charge to the customer's bank account. The recurring transaction information has been submitted and authorized and future payment will occur as scheduled.

NOTE:

- Any time that `pg_schedule_recurring_amount` is present, the total number of payments will be `pg_schedule_quantity` + 1. This takes into account that no transactions have been voided.
- A message containing a basic set of recurring fields will yield `pg_schedule_quantity` payments. This takes into account that no transactions have been voided.

2026 CSG Systems International and/or its affiliates ("CSG")

Understanding Response Messages

A transaction message can result in one of three possible outcomes: approved, declined, or error.

The three response fields (type, code, and description) give different levels of detail in all cases. Appendix A lists all the possible response codes for a transaction message, which can be classified into three groups: results, formatting errors, and exceptions.

The results group (codes beginning with“U”or“A”) represent successfully processed transactions (approved or declined). The formatting errors group (codes beginning with“F”) represent messages not processed because of one or more errors in the message formatting. The response description field will list the offending fields, and the original message is archived to assist in technical support. The exceptions group (codes beginning with“E”) represent codes for messages encountering some fatal condition preventing further processing (e.g., bad merchant ID, security error, or communications timeout).

The `preauth fields` are responses for EFT transactions utilizing the Forte Verify product. The `pg_preauth_result` field indicates the status of the account in question (see Appendix B for more information on Forte Verify processing).

2026 CSG Systems International and/or its affiliates (“CSG”)

Testing

The following section details what information you need to set up, test, certify, and bring your system up live with messages.

When testing on the Forte platform, consider:

- Our servers are available 24/7, every day
- You can build and test at your own pace
- We provide examples of code
- We provide preset responses for some messages so you will know what response indicates a successful test

After completing testing, your messages will be ready to be placed in a live production environment, and your system is ready for operation.

Preparing for Testing

Once you have composed your messages, you will need a system sign-on, which consists of a Merchant ID and processing password that should have been included in your new merchant approval letter/package.

Ports and URLs

The following table displays the port numbers used for testing the DSI delivery method.
The test URLs for the RAW HTTP POST and SOAP POST methods are also displayed:

Delivery Method	URL
DSI	Port 6050
HTTP POST	https://www.paymentsgateway.net/cgi-bin/posttest.pl
SOAP POST	https://ws.paymentsgateway.net/pgtest/paymentsgateway.asmx

Differences Between Test and Live Servers

The test and live servers are virtually the same except for the following differences:

- Test CC transactions are run through the authorizing vendors test system
- Test CC transactions are never settled
- Test EFT transactions are never settled
- Test recurring transactions are never processed
- Test Forte Verify transactions are run against an internal StarChek test bed

2026 CSG Systems International and/or its affiliates (“CSG”)

Going Live

"Going Live" occurs when your system is ready to work in a production environment. This step requires a minor change to your delivery method and a call to Forte to set up your live account.

To set up a live account contact Forte's Technical Support team.

The following table shows the parameters for live transactions:

Delivery Method	URL
DSI	Port 5050
HTTP POST	https://www.paymentsgateway.net/cgi-bin/postauth.pl
SOAP POST	https://ws.paymentsgateway.net/pg/paymentsgateway.asmx

2026 CSG Systems International and/or its affiliates ("CSG")

Best Practices

The following section summarizes best practices for integrating and maintaining Forte's platform.

Tools Available to Help You

Forte maintains the following online tools to help you through your integration:

Tool	Description	URL / Email
Knowledge Base	Search for answers to common questions	https://support.forte.net/support/home
Integration Support	Includes support for customers currently undergoing integration or needing assistance with integration or testing issues	mailto:intgration@forte.net
Developer Site	Includes sample code, a developer forum, and updated documentation	https://developers.forte.net/

Central Point of Contact

Forte recommends you route all communications through a designated central point-of- contact in your organization. This one person will have a full understanding of the business relationship and will keep Forte updated on important issues. Forte must be kept informed about any changes to messages, schedules, or issues that relate to Forte's platform.

Obtaining Help from Forte

When contacting Forte Technical Support, provide the following information to expedite your issue:

- Merchant ID
- Date of transaction in question
- Amount of transaction
- Name of purchaser

Managing Reconciliation Process

The reconciliation process is your responsibility. Failing to properly oversee this process can be costly.

With credit card transactions, you know immediately whether the transaction will be paid. However, with ACH and EFT transactions, settlement typically does not occur for a minimum of 3–4 days and with credit card chargebacks, settlement can take up to 90 days.

To mitigate the risk inherent in this long settlement time, you must reconcile your settlement information with your authorizations on a regular basis. You can obtain your settlement information from Forte and compare it to your authorizers. If you are pulling down EFT settlement information, a match against transaction results is a good way to ensure accuracy.

You can download settlement files from Forte's web site. For more information see the Batch Transmission File Specification available on DevDocs or via Virtual Terminal.

2026 CSG Systems International and/or its affiliates ("CSG")

Maintaining Documentation

Carefully documenting your integration helps make maintaining your system easier. Forte recommends you document the following:

- **Delivery Method**: Document why you chose that delivery method, who approved the delivery method, and the date you obtained the approval.
- **Messages**: Document the business purpose of each message, any alternate drafts considered, who approved the message, and the date you obtained the approval.
- **Testing**: Document the test methods you use (including any test scripts), who participated in the tests, who approved the test results, and the date you obtained the approval.
- **Certification**: If any changes are made to messages as a result of certification testing, be sure to adjust the documentation. If staff training is delivery during this phase, archive copies of the training materials. Also, you may wish to document who is trained and on what dates.
- **Go-Live**: Document all problems encountered during go-live (if any). Document individuals having problems with parts of the system (even if they were trained on how to use it because occasionally misunderstandings during training can occur).

If a problem occurs in a few months, this documentation will help you determine if the problem is new or was encountered when the system was integrated, tested, or put into production. Additionally, thorough documentation will help you determine whether users were ever trained on that topic.

2026 CSG Systems International and/or its affiliates (“CSG”)

2026 CSG Systems International and/or its affiliates (“CSG”)

Appendix A: Response Codes

The following section describes transaction response codes returned in the `pg_response_code` parameter of the response message.

Approved and Declined Responses

The following responses are returned for all processed transactions. The `A01` response is the only code ever returned for approved transactions. The `U` codes are for declined transactions. In some cases, the `pg_response_description` field value will differ from that in the Description column.

Code	Description	Comments	Test Parameters
A01	Approved	Transaction approved/completed	Example transaction messages in Appendix D
A03	Partial Authorization	Transaction approved for a partial authorization (Credit Card only)	Not available
A05	Overall match	The business name or full name provided exactly or closely matches the database record	
A06	Partial match	The full name or business name conditionally (partially) matches the database record	
N01	No info	The Routing and account numbers are found in the database, but no names are associated with these.	
U02	Account Not Approved	Customer account is in the Forte "Known Bad Accounts" list (EFT only)	Send echeck sale transaction with the following data: • Routing Number: `021000021` • Account Number: `987654321`
	TRN Not Approved	Routing number passes checksum test but is not valid for ACH	Send echeck sale transaction with the following data: • Routing Number: `064000101` • Account Number: Any Account Number
U03	Daily Trans Limit	Merchant daily limit exceeded (EFT only)	Not available
U04	Monthly Trans Limit	Merchant monthly limit exceeded (EFT only)	Not available
U05	AVS Failure ZIP Code	AVS State/ZIP Code check failed	Set `pg_avs_method=00200` and send a state and zip code that do not match
U06	AVS Failure Area Code	AVS State/Area Code check failed	Set `pg_avs_method=00200` and send a state and area code that do not match
U07	AVS Failure Email	AVS anonymous email check failed	Set `pg_avs_method=00200` and send an email address for Hotmail.com.

2026 CSG Systems International and/or its affiliates ("CSG")

Code	Description	Comments	Test Parameters
U08	DAILY VELOCITY	Merchant has exceeded the maximum number of transactions per hour, which may indicate a security problem. This error rarely occurs, but if you receive it,	
U09	WINDOW VELOCITY	Merchant has exceeded the maximum number of transactions per hour, which may indicate a security problem. This error rarely occurs, but if you receive it, contact Forte immediately.	
U10	Duplicate Transaction	Transaction has the same attributes as another transaction within the time set by the merchant	Send the same transaction twice within five minutes
U11	Recur Trans Not Found	Transaction types 40–42 only	Not Available
U12	Update Not Allowed	Original transaction cannot be voided or captured	Send a void transaction for a declined transaction
U13	Orig Trans Not Found	Transaction to be voided or captured was not found	Send void transaction for the following trace number: 00000000-0000-0000- 0000-000000000000
U14	Bad Type for Orig Trans	Void/Capture and original transaction types do not agree (CC/EFT)	Send a void credit card transaction for an echeck transaction
U15	Already Voided Already Captured	Transaction was previously voided or captured	Void the same transaction twice
U16	SETTLEMENT PROCESS STARTED	Void attempted after the start of the settlement process	
U18	Update Failed	Void or Capture failed	Send a transaction for $19.18 or $1918
U19	Invalid Trn	Account ABA number if is invalid	Send echeck transaction with TRN of 12345689
U20	Invalid Credit Card Number	Credit card number is invalid	Send a credit card transaction with a card number of 1111111111111111
U21	Bad Start Date	Date is malformed	Send a transaction with scheduling data but a start date of 13/1/2008 or 1/1/2001
U22	Swipe Data Failure	Swipe data is malformed	Send credit card transaction with ecom_payment_card_expdate_month =13
U23	Invalid Expiration Date	Malformed expiration date	Send credit card transaction with ecom_payment_card_expdate_month =13
U25	Invalid Amount	Negative Amount	Send a transaction for a negative amount (e.g., -$1.00)
U26	Invalid Data**	Invalid data present in the transaction	Send a void transaction with pg_original_authorization_code="".

2026 CSG Systems International and/or its affiliates ("CSG")

Code	Description	Comments	Test Parameters
U27	Conv Fee Not Allowed	Merchant configured for convenience fee but did not send one	For merchants configured to accept a convenience fee, send a transaction with an incorrect convenience fee in pg_convenience_fee
U28	Conv Fee Incorrect	Merchant configured for convenience fee but did not send one	For merchants configured to accept a convenience fee, send a transaction with an incorrect convenience fee in pg_convenience_fee
U29	Conv Fee Declined	Convenience fee transaction failed–SplitCharge model only	N/A
U30	Principal Declined	Principal transaction failed–SplitCharge model only	N/A
U32	Invalid Wallet Type	Invalid Wallet Type present in the transaction	Send a transaction with wallet type values out of ApplePay, GooglePay or SamsungPay
U33	Invalid Wallet Source	Wallet source is invalid	Send a transaction with wallet source values other than InApp, Web
U34	Invalid Wallet Cryptogram	Wallet cryptogram invalid. Length of cryptograms for different card brands: • Visa, Mast <= 28 characters • Disc, JCB, Diner <= 40 characters • Amex <= 56 characters	Send a transaction with digital wallet cryptogram. Where Length of cryptograms for different card brands is not as show below: • Vis , Mast <= 28 characters • Disc, JCB, Diner <= 40 characters • Amex <= 56 characters
U35	Incorrect Market Type	Market type must be ecommerce for digital wallet transcations	N/A
U36	SURCHARGING NOT SUPPORTED	Merchant sent a surcharge fee but is not configured to accept one	N/A
U37	CFEE AMT EXCEEDED	The "Convenience Fee amount" of the refund transaction is exceeding its respective amount in the original sale transaction.	**Send a refund transaction for 1.75 or 175** **Note:** The Service_fee_amount field, if prov ided, should match the service_fee_amount **configured for the location.**
U38	SUBTOTAL AND TAX AMT EXCEEDED	The "Subtotal & tax amount" of the refund transaction exceeds its respective amount in the original sale transaction.	Send a refund transaction for 1.76 or 176 **Note**: The Service_fee_amount field, if prov ided, should match the service_fee_amount configured for the location.
U39	ORIGINAL AUTHORIZED AMOUNT EXCEEDED	Both “Convenience Fee amount” & "Subtotal & tax amount” of the refund transaction is excee ding their respective amounts i n the original sale transaction.	Send a refund transaction for 1.77 or 177 **Note**: The Service_fee_amount field, if prov ided, should match the service_fee_amount configured for the location.

2026 CSG Systems International and/or its affiliates (“CSG”)

Code	Description	Comments	Test Parameters
U40	REFUND CURRENTLY IN PROGRESS	If two refunds are processed at the same time, the latest transaction will be declined with this error message.	Send a refund transaction for 1.78 or 178 **Note**: The Service_fee_amount field, if prov ided, should match the service_fee_amount configured for the location.
U41	REFUNDS APPLY ONLY TO SETTLED/SETTLIN G/ FUNDED TRNASACTIONS	Refund is applicable only if the original sale transaction status is Settled/ Settling/ Funded. Fo r any case where the status is NOT Settled/ Settling/ Funded when attempting a refund, it wil l be declined with this error me ssage.	Send a refund transaction for 1.79 or 179 **Note**: The Service_fee_amount field, if prov ided, should match the service_fee_amount configured for the location.
U42	SURCHARGE FEE INCORRECT	Merchant configured for surcharge fee but did not send one	N/A
U43	SURCHARGE AMOUNT INCORRECT	The "Surcharge Fee amount" of the refund transaction is exce eding its respective amount in the original sale transaction.	N/A
U51	Merchant Status	Merchant is not“live”	Send a transaction for a non-live Merchant ID
U52	Type Not Allowed	Merchant not approved for transaction type (Credit Card or EFT)	Send a transaction of a type (credit card or echeck) that the account is not allowed to process
U53	Per Trans Limit	Transaction amount exceeds merchants per transaction limit (EFTs only)	Send a transaction that exceeds the merchant’s echeck limit(s)
U54	Invalid Merchant Config	Merchant’s configuration requires updating–call Customer Support	Send a transaction for $19.54 or $1954
U56	CARD TYPE NOT ALLOWED	Your merchant account does not support the provided credi t card brand. Call Customer Service at 1-866-290-5400 to update your merchant configuration settings.	
U57	Digital wallet not configured	Merchant is not configured for digital wallets, but the request is populated with wallet specific fields	N/A
U58	Specific Wallet type not configured	Merchant is not configured for a specific wallet type, but the request has it	N/A
U59	Incorrect Wallet configuration	Merchant is incorrectly configured to accept wallet payments, but the processor does not support digital wallets	N/A

2026 CSG Systems International and/or its affiliates (“CSG”)

Code	Description	Comments	Test Parameters	
U77	Device or Application No Longer Supported	Returns when the pg_response_description indicates that the client device or application version is deprecated and no longer supported by the payment gateway.	N/A	
U78	Disallowed ACH SEC Code	Indicates that the SEC code passed in with the ACH transaction is not allowed for the merchant account	Send a transaction with SEC code“XYZ”	
U79	CARD NOT HONORED	Allowed On a high level this error is returned when the provided BIN is blocked from processing. Bin is restricted from processing based on one of the following rules: • Merchant Level - Bin is blocked for the merchant. • Source Level - Bin is blocked for specific transaction source. • Country Level - Bin is blocked based on originating country • Global Level - Bin is Blocked across all merchants (Company-wide)		
U80	Preauth Decline	Transaction was declined due to Preauthorization (Forte Verify) result	Send a transaction for $19.80 or $1980	
U81	Preauth Timeout	Preauthorizer not responding (Verify Only transactions)	Send a transaction for $19.81 or $1981	
U82	Preauth Error	Preauthorizer error (Verify Only transactions only)	Send a transaction for $19.82 or $1982	
U83	Auth Decline*	Transaction was declined due to authorizer declination	Send a transaction for $19.83, $1983, or $1.33	
U84	Auth Timeout	Authorizer not responding	Send a transaction for $19.84 or $1984	
U85	Auth Error	Authorizer error	Send a transaction for $19.85 or $1985	
U86	AVS Failure Auth	Authorizer AVS check failed	Send a transaction for $19.86 or $1986	
U87	Auth Busy	Authorizing vendor busy, may be resubmitted (credit card only)	Send a transaction for $19.87 or $1987	
U88	Preauth Busy	Verification vendor busy, may be resubmitted (type 26 only)	Send a transaction for $19.88 or $1988	
U89	Auth Unavail	Vendor service unavailable (credit card only)	Send a transaction for $19.89 or $1989	
U90	Preauth Unavail	Verification service unavailable (type 26 only)	Send a transaction for $19.90 or $1990	

2026 CSG Systems International and/or its affiliates (“CSG”)

Code	Description	Comments	Test Parameters
U91	Credit Card Not Allowed	Merchant accounts are configured to process only Debit Cards. Credit Cards are not allowed.	N/A
U92	Debit Card Not Allowed	Merchant account is configured to process only Credit Cards. Debit cards not allowed	N/A
U93	DECRYPT INPUT ERROR	Caused by an error during the decryption	Send the same encrypted card data twice.

**pg_response_description will contain the text of the vendor's response.*
***pg_response_description will contain a more specific message.*

Formatting Error Responses

The following table displays the codes returned when Forte finds formatting errors. The response description field will list all the offending fields in the message (to the 80-character limit). The description field will be formatted as:
`<code>:<fieldname>[,<code>:<fieldname>  ...]`
The `pg_response_code` will contain the first error type encountered. All formatting errors begin with an "F."

Code	Description	Comments
F01	Mandatory Field Missing	Required field is missing
F03	Invalid Field Name	Name is not recognized
F04	Invalid Field Value	Value is not allowed
F05	Duplicate Field	Field is repeated in message
F07	Conflicting Field	Fields cannot both be present

Fatal Error Responses

The following table displays exceptions that will stop the processing of a well-formed message due to security or other considerations. All fatal exceptions begin with an "E."

Code	Description	Comments
E10	Invalid Merchant or Password	Merchant ID or processing password is incorrect
E20	Merchant Timeout	Transaction message not received (I/O flush required?)
E55	Invalid Token	Specified token was invalid, could not be located, or may have been deleted
	Client Token Transactions	For client token transactions where neither payment fields nor a payment token were specified, the client record does not have a default payment method matching the transaction type
	Payment Token Transactions	For payment token transaction where no client token is specified, the payment token must be clientless
	Both Client and Payment Tokens Present	For transactions with client and payment tokens, the specified payment token is not associated with the client or is clientless
E90	Bad Merch IP Addr	Origination IP not on merchant's approved IP list
E99	Internal Error	An unspecified error has occurred

2026 CSG Systems International and/or its affiliates ("CSG")

Appendix B: Forte Verify

Forte Verify is an optional service that provides additional verification of an EFT account number. Forte performs these "preauthorization" searches (also called "checks") automatically for subscribing merchants (the authorization messages require no additional fields).

Verifying Accounts

The Forte Verify service consults the status reported by the bank to see if the customer account is valid and in good standing. The response indicates if the account is open and valid, closed, NSF, or one of the other conditions listed in the table below. Charges are only assessed for transactions involving participating banks (Most Tier I and II banks participate, but some local banks and smaller credit unions may not). Transactions that do not receive a definitive response (such as `POS` or `NEG`) may then be checked against the national negative check database. Note that the status of the account may change between the bank's report and settlement.

Using Forte Verify

Forte Verify searches yield up to four additional response fields (see below). The most important field is `pg_preauth_result`, which indicates the result of the verification. `POS` indicates a positive response from the verification service and `NEG` indicates a negative response. `UNK` indicates that nothing more is known about the account (for various reasons). Use the following response fields when performing Forte Verify searches:

- `pg_preauth_result` - The value in this field may cause a transaction to be declined, depending upon the setup. Potential values for this field include the following: `POS`, `NEG`, or `UNK`.
- `pg_preauth_description` - This field displays the current state of the account as provided by the verifying agent.
- `pg_preauth_neg_report` - This field indicates negative database responses and normally contains the negative report details and (usually) the name and phone number of the reporting entity.

Response Values

Forte returns the following values in the result and description fields listed above. Sandbox normally generates a `POS` result for any account (no participating bank check is performed).
The test account numbers below may be used on Sandbox (with any valid ABA number) to force the indicated response.

Result	Description	Test Account #
NEG	P15: HIGH RISK	99915
NEG	P41: NEGATIVE INFO	99941
UNK	P50: NO INFO	99950
POS	P70: VALIDATED	99970
POS	P71: LOW RISK APPROVAL	99971
POS	P73: MEDIUM RISK APPROVAL	99973
UNK	P80 PREAUTH VENDOR BUSY	99980
UNK	P90: PREAUTH VENDOR UNAVAIL	99990
UNK	P91: PREAUTH VENDOR ERROR	99991
UNK	P92: PREAUTH SERVER UNAVAIL	99992

2026 CSG Systems International and/or its affiliates ("CSG")

Approval and Forte Verify

Forte Verify applies only to Sales, Auth Only, and Verify Only transactions (Types `20`, `21`, and `26`). Transactions with a `NEG` result are normally declined for that reason. Those with `UNK` and `POS` responses are not declined and may be subject to other checks. Normally, `UNK` and `POS` responses are approved. If the merchant only uses Verify Only transactions, he or she may want to use the `pg_preauth_result` value instead of the `pg_response_type` value for his/her decision making.

Authorization and Forte Verify

Within the Forte platform, merchants can set up multiple levels of account verification for ACH items. If the final response is positive, `UNK`, or the account is not found, the transaction is APPROVED in all cases. If the final response has negative reports, the transaction is DECLINED.

2026 CSG Systems International and/or its affiliates (“CSG”)

Appendix C: Authenticate:

Authenticate is an optional service that provides bank account owner name verification of an EFT account number. This service supports instant verification for all participating banks.

Ownership Verification

Authenticate service validates if the account owner name or business name matches what the bank has for the given account number. The response indicates if the specified name fields are an exact match or a partial match. Charges are only assessed for inquiries involving participating banks (Most Tier I and II banks participate, but some local banks and smaller credit unions may not). Ownership verification can be made by passing ecom_billto_postal_ name_first and ecom_billto_postal_ name_last, pg_billto_postal_ name_company or all 3 fields in the transaction message.

Using CSG Forte Authenticate:

When using the CSG Forte Authenticate service the transaction response has as few additional fields (see below). The most important field is pg_preauth_result which indicates the result of ownership verification. `POS` indicates a good match on ownership, `CON` indicates partial match and `NEG` indicates no match. Ownership verification is applicable only to Authenticate Only transaction (pg_transaction_type='`26`' and pg_transaction_subtype='`authenticate`')

Response Fields:

- `pg_preauth_result` - The value in this field provides the match result. Potential values for this field include the following: `POS, NEG, CON, UNK, ERROR`.
- `pg_preauth_description` - This field displays the current state of the account ownership match as provided by the verifying agent. Potential values for this field include the following:
  - P60: MATCH, P10: NO MATCH, P75: CONDITIONAL MATCH
- `pg_response_description` - This value provides additional information on the match. Potential values are outlined below.
  - `OVERALL MATCH`– First name, Last name and Business Name are a match
  - `FIRST & LAST NAME MATCH`– First name and Last name are a match
  - `BUSINESS NAME MATCH`– Business name is a match
  - `PARTIAL MATCH`– At least one name field matched and at least one name field didn't match
  - `NO INFO` - Ownership information is not available (In case of non-participating bank)
- `pg_ownership_match` = This field provides pipe delimited results of match results for name fields being inquired upon. Potential values are `Y, N, C, U` (`Y`-Match, `N`-No Match, C-Conditional Match `U`-No Info)
- `FirstNameMatch|LastNameMatch|NameMatch|BusinessNameMatch`
- `pg_response_type` – This field provides type of response generated by authenticate - Overall match
  - M - FirstName/LastName match
  - B - Business name match
  - P - Conditional match
  - N - No match
  - U - No Info
  - E - Timeout or Invalid response/internal error or Bad request

2026 CSG Systems International and/or its affiliates ("CSG")

Response Values:
Authenticate service returns the following values in the result and description fields listed above (no participating bank check is performed).

The test account numbers mentioned in the below table may be used on Sandbox (with any valid ABA number) to force the indicated response.

PG_PREAUTH_CODE	PG_PREAUTH_RESULT	PG_PREAUTH_DESCRIPTION	PG_RESPONSE_CODE	PG_RESPONSE_DESCRIPTION	PG_RESPONSE_TYPE	PG_OWNERSHIP_MATCH	SANDBOX TEST DDA
P60	POS	MATCH	A05	OVERALL MATCH	O	Y|Y|Y|Y	99801
P60	POS	MATCH	A05	FIRST & LAST NAME MATCH	M	Y|Y|Y|	99802
P60	POS	MATCH	A05	FIRST & LAST NAME MATCH	M	Y|Y|Y|N	99803
P60	POS	MATCH	A05	BUSINESS NAME MATCH	B	|||Y	99804
P60	POS	MATCH	A05	BUSINESS NAME MATCH	B	N|N|N|Y	99805
P10	NEG	NO MATCH	U80	NO MATCH	N	N |N |N|N	99806
P10	NEG	NO MATCH	U80	NO MATCH	N	N |N |N|	99807
P10	NEG	NO MATCH	U80	NO MATCH	N	|||N	99808
P75	CON	CONDITIONAL MATCH	A06	PARTIAL MATCH	P	Y|Y|Y|C	99809
P75	CON	CONDITIONAL MATCH	A06	PARTIAL MATCH	P	N|Y|N|Y	99810
P75	CON	CONDITIONAL MATCH	A06	PARTIAL MATCH	P	N|Y|N|N	99811
P75	CON	CONDITIONAL MATCH	A06	PARTIAL MATCH	P	N|Y|N|C	99812
P75	CON	CONDITIONAL MATCH	A06	PARTIAL MATCH	P	N|Y|N|	99813
P75	CON	CONDITIONAL MATCH	A06	PARTIAL MATCH	P	Y|N|N|Y	99814
P75	CON	CONDITIONAL MATCH	A06	PARTIAL MATCH	P	Y|N|N|N	99815
P75	CON	CONDITIONAL MATCH	A06	PARTIAL MATCH	P	Y|N|N|C	99816
P75	CON	CONDITIONAL MATCH	A06	PARTIAL MATCH	P	Y|N|N|	99817
P75	CON	CONDITIONAL MATCH	A06	PARTIAL MATCH	P	N|N|N|C	99818
P75	CON	CONDITIONAL MATCH	A06	PARTIAL MATCH	P	|||C	99819
P50	UNK	NO INFO	N01	NO INFO	U	|||	99820
P90	UNK	PREAUTH VENDOR UNAVAIL	U84	AUTH TIMEOUT	E	|||	99821
P91	UNK	PREAUTH VENDOR ERROR	U82	PREAUTH ERROR	E	|||	99822
P91	UNK	PREAUTH VENDOR ERROR	U85	AUTH ERROR	E	|||	99823
P94	NEG	INVALID ROUTING NUMBER	U19	Invalid Routing/Transit number INV	I	|||	99824
P94	NEG	INVALID ACCOUNT NUMBER	U02	Invalid Account number INV	I	|||	99825

2026 CSG Systems International and/or its affiliates (“CSG”)

P95	NEG	BAD ACCOUNT	U80	N/A	E	|||	99826
P94	ERROR	INVALID ROUTING NUMBER	U19	Invalid Routing/Transit number INV	I	|||	99827
P94	ERROR	INVALID ACCOUNT NUMBER	U80	Invalid Account number INV	I	|||	99828
P94	ERROR	INVALID ACCOUNT NUMBER LENGTH	U80	Account Number length error	I	|||	99829

2026 CSG Systems International and/or its affiliates (“CSG”)

Appendix D: AVS and Other Verification Systems

Credit card companies typically use Address Verification Systems (AVS) by matching the street address number and the zip code with that of the cardholder.
Forte offers more verification checks, including the following:

- State/Zip Code match
- State/Area Code match
- Anonymous Email check

The `pg_avs_method` field specifies what checks to perform and whether to decline a transaction if they fail. The `pg_avs_results` field indicates which checks passed, failed, or were not performed. Both fields consist of five digits, each representing one of the checks mentioned above.

The table below lists the checks represented by each digit position. X1 X2 X3 X4 X5 is the value specified by one of the AVS fields:

Digit	Description
X1	Credit Card Account/Zip Code Check
X2	Credit Card Account/Street Number Check
X3	State/ZIP Code Check
X4	State/Area Code Check
X5	Anonymous Email Check

The digits represent different values depending on the field:

Digit	pg_avs_method	Digit	pg_avs_result
0	Do not perform check	0	Check not performed
1	Check only; do not decline on fail	3	Passed
2	Check and decline on fail	4	Failed

Forte only performs Credit Card Account checks for credit card transactions and ignores EFT transactions. The merchant's assigned authorizing agent (e.g., Nova) performs the checks. The authorizer authorizes the transaction if the AVS checks fail and there is no other reason to decline. If the `pg_avs_method` position representing a failed check is set to 2, the processor declines the transaction and it will not settle.

NOTE:

- Forte recommends that merchants at least have these checks performed (positions 1 and 2 set to 1) as they will usually get a better rate from the authorizer.
- State/ZIP Code and State/Area Code Checks (Positions 3 and 4)
- The State/Zip Code and State/Area Code checks compare the customer's billing address state (official two-character abbreviation) and zip code or area code.

2026 CSG Systems International and/or its affiliates ("CSG")

Anonymous Email Check (Position 5)

The Anonymous Email check compares the customer's specified email address against a list of known anonymous email services (e.g., Hotmail).

The following table displays examples of Anonymous Email checks:

Method	Results	Declined?	Description
22000	34000	Yes	Declined because the Credit Card Street Number check failed
11000	34000	No	The Credit Card Street Number check failed, but the action was a "Check Only"
22001	33004	No	The Anonymous Email check failed, but the action was a"Check Only"
00222	00334	Yes	The Anonymous Email check failed and was a "Decline on Fail" action

NOTE: If the required data for a requested AVS check (value of"1"or"2")is missing, Forte sends an `F01` (mandatory field missing) response code along with the missing field(s).

Implicit AVS Checks

Forte still performs an AVS check even if the merchant specifies the zip code and/or street address fields for a credit card transaction without specifying the `pg_avs_method` field. Forte performs this implicit AVS check silently without returning the `pg_avs_result` field.

2026 CSG Systems International and/or its affiliates ("CSG")

Appendix E: Example Messages

The following sections illustrate various message types. Each message is displayed as newline delimited and the merchant ID and password values have been omitted. A newline character is present after the `endofdata` tag in each of the messaging examples.

Credit Card Sale Transaction

```
pg_merchant_id=<Merchant ID>
pg_password=<Merchant
Password>
pg_transaction_type=10
pg_total_amount=1.13
ecom_billto_postal_name_firs
t=John
ecom_billto_postal_name_last
=Smith
ecom_billto_postal_street_line1=123 Any
Street ecom_billto_postal_city=San Diego
ecom_billto_postal_stateprov=CA
ecom_billto_postal_postalcode=92104
ecom_payment_card_name=John Smith
ecom_payment_card_type=Visa
ecom_payment_card_number=<Credit Card
Account Number>
ecom_payment_card_expdate_month=<Credit Card
Expiration Month>
ecom_payment_card_expdate_year=<Credit Card
Expiration Year> pg_avs_method=22000
endofdata
```

Credit Card Capture Transaction

```
pg_merchant_id=<Merchant ID>
pg_password=<Merchant
Password>
pg_transaction_type=12
pg_original_authorization_cod
e=42344
pg_original_trace_number=c3dce169-ad27-
11d5-a75c- 0050da8def0f
endofdata
```

Credit Card Authorize Only Transaction

```
pg_merchant_id=<Merchant ID>
pg_password=<Merchant Password>
pg_transaction_type=11
pg_total_amount=1.00
ecom_billto_postal_name_first=John
ecom_billto_postal_name_last=Smith
ecom_billto_postal_street_line1=123 Any Street
ecom_billto_postal_city=San Diego
```


2026 CSG Systems International and/or its affiliates (“CSG”)

```
ecom_billto_postal_stateprov=CA
ecom_billto_postal_postalcode=92104
ecom_payment_card_name=John Smith
ecom_payment_card_type=Visa
ecom_payment_card_number=<Credit Card Account Number>
ecom_payment_card_expdate_month=<Credit Card Expiration Month>
ecom_payment_card_expdate_year=<Credit Card Expiration Year>
pg_avs_method=22000
endofdata
```

Credit Card Force Transaction

```
pg_merchant_id=<Merchant ID>
pg_password=<Merchant Password>
pg_transaction_type=15
pg_total_amount=1.13
ecom_billto_postal_name_first=John
ecom_billto_postal_name_last=Smith
ecom_billto_postal_street_line1=123 Any Street
ecom_billto_postal_city=San Diego
ecom_billto_postal_stateprov=CA
ecom_billto_postal_postalcode=92104
ecom_payment_card_name=John Smith
ecom_payment_card_type=Visa
ecom_payment_card_number=<Credit Card Account Number>
ecom_payment_card_expdate_month=<Credit Card Expiration
Month>
ecom_payment_card_expdate_year=<Credit Card Expiration
Year>
pg_original_authorization_code=42344
endofdata
```

Credit Card Recurring Sale (Initial Charge + 11 Equal Monthly Charges)

```
pg_merchant_id=<Merchant ID> pg_password=<Merchant
Password> pg_transaction_type=10 pg_total_amount=9.95
ecom_billto_postal_name_first=John
ecom_billto_postal_name_last=Smith
ecom_billto_postal_street_line1=123 Any Street
ecom_billto_postal_city=San Diego
ecom_billto_postal_stateprov=CA
ecom_billto_postal_postalcode=92104
ecom_payment_card_name=John Smith
ecom_payment_card_type=Visa
ecom_payment_card_number=<Credit Card Account Number>
ecom_payment_card_expdate_month=<Credit Card Expiration
Month>
ecom_payment_card_expdate_year=<Credit Card Expiration
Year>
pg_avs_method=22000
pg_schedule_frequency=20 pg_schedule_quantity=12
endofdata
```


2026 CSG Systems International and/or its affiliates (“CSG”)

EFT Sale Transaction

```
pg_merchant_id=<Merchant ID> pg_password=<Merchant
Password> pg_transaction_type=20 pg_total_amount=10.00
ecom_billto_postal_name_first=John
ecom_billto_postal_name_last=Smith
ecom_billto_postal_street_line1=123 Any Street
ecom_billto_postal_city=San Diego
ecom_billto_postal_stateprov=CA
ecom_billto_postal_postalcode=92104
ecom_payment_check_account_type=S
ecom_payment_check_account=<Account Number>
ecom_payment_check_trn=<Routing Number>
pg_avs_method=00220
endofdata
```

EFT Verify Only Transaction

```
pg_merchant_id=<Merchant ID> pg_password=<Merchant
Password> pg_transaction_type=26 pg_total_amount=10.00
ecom_payment_check_account_type=S
ecom_payment_check_account=<Account Number>
ecom_payment_check_trn=<Routing Number> endofdata
```

EFT Void Transaction

```
pg_merchant_id=<Merchant ID> pg_password=<Merchant
Password> pg_transaction_type=24
pg_original_authorization_code=42344
pg_original_trace_number=c3dce169-ad27-11d5-a75c-
0050da8def0f endofdata
```

Recurring Admin Delete Transaction

```
pg_merchant_id=<Merchant ID> pg_password=<Merchant
Password> pg_transaction_type=42
pg_original_trace_number=ef0fe169-ad27-11d5-a75c-
c3dc0050da8d endofdata
```

EFT Sale Transaction Response (with Forte Verify)

```
pg_response_type=A pg_response_code=A01
pg_response_description=APPROVED
pg_merchant_id=<Merchant ID>
pg_authorization_code=420023
pg_trace_number=f0b77189-4014-11d6-a7fd- 0050da8def0f
pg_avs_result=0330 pg_transaction_type=20
pg_total_amount=25.95
ecom_billto_postal_name_first=John
ecom_billto_postal_name_last=Smith pg_preauth_code=none
pg_preauth_result=POS
pg_preauth_description=P70:VALIDATED endofdata
```


2026 CSG Systems International and/or its affiliates (“CSG”)

Glossary

ACH
The Automated Clearing House is a national network for batch-oriented electronic funds transfer. ACH transactions are governed by NACHA operating rules and provide a method for transferring funds between banks using the Federal Reserve System. Most (but not all) financial institutions use the ACH network.
The types of ACH payments include the following:

- Direct deposits of all types including tax refunds, payroll and government benefits (e.g., Social Security)
- Direct payments of bills such as utilities, mortgages, loans, and insurance policies
- Federal, state, and local tax payments
- Business-to-business payments
- eChecks
- eCommerce payments

Approval
An approval is any transaction approved by the credit provider or the check writer's bank. Approvals are granted after an authorization has been requested by a merchant.

Authorization
Only used for credit card transactions. An authorization is a request from a merchant to charge a cardholder. If approved, the authorization will decrease the customer's available credit, but will not actually capture any funds. An authorization is the first step in the delayed settlement process where the merchant may obtain an approval, but if it is not settled within a specific period of time, the authorization will expire. The credit provider determines the delay period.

Authorization Code
Numeric or alphanumeric code issued by the credit provider and used to reference the authorization.

Auth Only
In this type of authorization, the merchant does not intent to capture funds until a later date. Often, funds are not captured on these authorizations.

Capture
Refers to the "capture" of funds at the end of a transaction. This typically follows "settlement" of the transaction, where the amount is actually debited to the customer's account.

Decline
A transaction which is not approved by the credit provider/issuer. No authorization is issued.

DSI
Direct Socket Interface (DSI) is Forte's recommended delivery method. This is the native method for the Forte platform and is a Secure Sockets Layer connection.

2026 CSG Systems International and/or its affiliates ("CSG")

EFT
Electronic Funds Transfer (EFT) provides for electronic payments and collections. EFT is safe, secure, efficient, and less expensive than paper check payments and collections. EFT is the preferred method of payment for the government. As stated by the Treasury web site“itcosts the U.S. government $.83 to issue each check payment, it costs only $.08 to issue an EFT payment.”

Merchant ID
This is the identification number for your organization, used by Forte to identify you in all communications. It is critical that anyone contacting Forte for assistance know this ID number.

Pre Auth
This has the same meaning as Auth Only.

Pre-Notification
Prior to sending the first ACH transaction to an ACH receiver or the ACH receiver’s account, the ACH originator may (optionally) send a pre-notification to be processed to the customer’s account. This provides notice of the intent to send additional items and the date on which they will be drafted from the customer’s account.

Procurement Card
Like credit cards and gift cards, procurement cards are typically issued by organizations to enable employees to purchase supplies or items for company use.

RAW
In computer terminology, this refers to unprocessed data. This term came originally from the UNIX platform and generally refers to data that is passed along without being interpreted or processed in any way.

Reversal
If a transaction has already settled and should have been voided, it can be reversed by issuing a credit to correct the error.

Settlement
In this process, authorized transactions are sent to the processor for payment to the merchant. This process finalizes the transaction and allows funds due the merchant to be“captured” and routed to the merchant’s bank for deposit. (In other words, the merchant cannot be paid until the transaction is settled.) It can take several days for funds to reach settlement.
Credit card settlement may be within one day, while settlement for checks may take up to 90 days.

SIC
Acronym for Standard Industry Classification, this four-digit code is used to classify types of businesses and industries.

2026 CSG Systems International and/or its affiliates (“CSG”)

SSL

SSL is an acronym for Secure Sockets Layer, a communications protocol used to transmit private documents or information via the Internet. SSL encrypts data using a private key that is transferred over the SSL connection. Web sites that require an SSL connection have an address that begins with *https://* rather than *http://*.

Travel and Entertainment Card

These credit cards usually require payment in full every month (e.g., American Express, Diner's Club and Carte Blanche).

Void

To void a transaction is to cancel one that has been authorized, but not yet settled. Settled transactions may not be voided, they must be reversed.

2026 CSG Systems International and/or its affiliates ("CSG")