

Release Notes



Cybersource Contact Information

For general information about our company, products, and services, go to <https://www.cybersource.com>.

For sales questions about any Cybersource service, email sales@cybersource.com or call 650-432-7350 or 888-330-2300 (toll free in the United States).

For support information about any Cybersource service, visit the Support Center: <https://www.cybersource.com/support>

Copyright

© 2020. Cybersource Corporation. All rights reserved. Cybersource Corporation ("Cybersource") furnishes this document and the software described in this document under the applicable agreement between the reader of this document ("You") and Cybersource ("Agreement"). You may use this document and/or software only in accordance with the terms of the Agreement. Except as expressly set forth in the Agreement, the information contained in this document is subject to change without notice and therefore should not be interpreted in any way as a guarantee or warranty by Cybersource. Cybersource assumes no responsibility or liability for any errors that may appear in this document. The copyrighted software that accompanies this document is licensed to You for use only in strict accordance with the Agreement. You should read the Agreement carefully before using the software. Except as permitted by the Agreement, You may not reproduce any part of this document, store this document in a retrieval system, or transmit this document, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written consent of Cybersource.

Restricted Rights Legends

For Government or defense agencies: Use, duplication, or disclosure by the Government or defense agencies is subject to restrictions as set forth in the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in similar clauses in the FAR and NASA FAR Supplement.

For civilian agencies: Use, reproduction, or disclosure is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights clause at 52.227-19 and the limitations set forth in Cybersource Corporation's standard commercial agreement for this software. Unpublished rights reserved under the copyright laws of the United States.

Trademarks

Authorize.Net, eCheck.Net, and The Power of Payment are registered trademarks of Cybersource Corporation. Cybersource, Cybersource Payment Manager, Cybersource Risk Manager, Cybersource Decision Manager, and Cybersource Connect are trademarks and/or service marks of Cybersource Corporation. Visa, Visa International, Cybersource, the Visa logo, and the Cybersource logo are the registered trademarks of Visa International in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Confidentiality Notice

This document is furnished to you solely in your capacity as a client of Cybersource and as a participant in the Visa payments system.

By accepting this document, you acknowledge that the information contained herein (the "Information") is confidential and subject to the confidentiality restrictions contained in Visa's operating regulations and/or other confidentiality agreements, which limit our use of the Information. You agree to keep the Information confidential and not to use the Information for any purpose other than its intended purpose and in your capacity as a customer of Cybersource or as a participant in the Visa payments system. The Information may only be disseminated within your organization on a need-to-know basis to enable your participation in the Visa payments system. Please be advised that the Information may constitute material non-public information under U.S. federal securities laws and that purchasing or selling securities of Visa Inc. while being aware of material non-public information would constitute a violation of applicable U.S. federal securities laws.

Revision

Version: 2

Contents

Release Notes.....	4
Announcements.....	5
Features Introduced This Week.....	7
Fixed Issues.....	8
Known Issues.....	9

Release Notes

These release notes cover all releases to the production server for the week ending November 29, 2024.

Announcements

Important: SOAP Toolkit Update

As part of ongoing security enhancements, we are planning to upgrade SOAP API authentication to P12 authentication. This upgrade is currently available for Java, C++, C#, and PHP. For instructions, read the [P12 Authentication Upgrade for SOAP Keys Migration Guide](#).

SSL/TLS Certification Migration

To uphold the maximum levels of security and compliance in both your browser-based and server-to-server interactions with the Visa Acceptance Solutions platform (including Cybersource), we are transitioning all Cybersource endpoint SSL/TLS certificates from Entrust to DigiCert. These SSL/TLS certificates, originally issued by Entrust, will now be issued by DigiCert to fortify these communication channels.

Merchants using Cybersource endpoints should coordinate with their network team or hosting/solution provider to implement all necessary measures to ensure their connections to Cybersource properties follow industry standards. This includes updating their systems with the new Root and Intermediate (CA) SSL/TLS certificates that correspond to the specific Cybersource endpoint they use.

If your application requires trusting of certificates at the server level, you must install (trust) the new certificates prior to expiration of existing certificates to avoid any production impact. The link to the Server-Level (leaf) SSL certificate will be updated when they become available.



Important

We recommended that merchants trust only the Root and Intermediate CA SSL/TLS certificates on all secure endpoints. This method avoids the annual necessity to renew the server-level certificate.

Do not revoke or remove any of your existing Entrust certificates linked with Cybersource endpoints before the scheduled dates. Until the cut-off dates, the only supported certificates will be the Entrust SSL certificates. You may add the new certificates to your

system, in addition to the existing certificates, and verify their functionality in the testing environment.

There will be two phases and each phase will update different endpoints.

First Phase

The first phase is complete and updated the following endpoints:

Test URLs	Production URLs
apitest.cybersource.com	accountupdater.cybersource.com
accountupdatertest.cybersource.com	api.cybersource.com
batchtest.cybersource.com	batch.cybersource.com
api.accountupdatertest.cybersource.com	api.accountupdater.cybersource.com
ics2wstest.ic3.com	ics2ws.ic3.com
ics2wstesta.ic3.com	ics2wsa.ic3.com
apitest.cybersource.com	ics2ws.in.ic3.com
	api.in.cybersource.com
	batch.in.cybersource.com

The new certificates can be found in the zip file at [this link](#).



Important

We strongly urge you to test your implementation as soon as possible.

Second Phase

The second phase will update the following endpoints:

Test URLs	Production URLs
testflex.cybersource.com	flex.cybersource.com
testsecureacceptance.cybersource.com	secureacceptance.cybersource.com
	flex.in.cybersource.com
	secureacceptance.in.cybersource.com

The Testing Environment was updated November 5, 2024, 4:00 GMT. The production environment December 10, 2024, 4:00 GMT. The old certifications will expire on December 31, 2024.

Features Introduced This Week

No customer-facing features were released this week.

Fixed Issues

No customer-facing fixes were released this week.

Known Issues

Decision Manager

Description

Users who do not have administrator permissions in the Business Center may be unable to see some negative list hyperlinks under Decision Manager > Case Management > Model Results, and in Transaction Management > Transaction > Transaction Details.

Audience

Merchants using Decision Manager to review orders.

Technical Details

None.

Workaround

None.

Merchant Boarding | 1614572

Description

Some users of the VAP Portfolio might be able to set up new gateways for existing merchant accounts, which can cause transaction failure.

Audience

Merchants who use the Business Center's Merchant Management feature to configure Merchant accounts using the Card Processing template.

Technical Details

If a user who does not have the Template Edit permission edits the card processing configuration of an existing Merchant ID by adding a new gateway, our internal gateway selector might not send transactions to the expected gateway.

Workaround

Ensure that the Template Edit permission is given to all users who configure merchant accounts in the Business Center.

API Response Codes | 1561217**Description**

A defect is causing transactions for pre-paid non-reloadable cards that are approved by Worldpay to be declined by our system due to invalid response code mapping.

Audience

Merchants who process transactions for pre-paid non-reloadable cards using Worldpay.

Technical Details

None.

Workaround

None.

Subscription Payments | 1573208**Description**

When a zero-amount authorization is included in a subscription creation request, the request results in failure for American Express, Discover, Diners, JCB, and CUP transactions.

Audience

Merchants processing on FDC Nashville and performing Token Creation calls without a Full Auth Amount.

Technical Details

This defect results in reason code 102: DINVALIDDATA with description \$0 auth not supported for [Card Scheme] on this gateway.

Workaround

- If you are tokenizing your customers before they place an order, create a token in conjunction with a \$1 Authorization then perform a full authorization reversal to remove the temporary funding block on your customer account.
- If you are tokenizing your customers at time of checkout, create a token in conjunction with the full amount of the customer's order.

Virtual Terminal | 1588256

Description

A defect is preventing Level III transactions in Virtual Terminal when Level II fields are set as required fields, even when all required fields are included.

Audience

Users of Virtual Terminal who perform Level III transactions.

Technical Details

The user receives the error message: Level2PurchaseOrderNumber is a required field.

Workaround

Use the API instead of Virtual Terminal.

Payments | 1560940

Description

A defect is causing payment transactions with an incorrect Card Verification Value (CVV) to receive a response code that claims the transaction can still be captured. However, capture fails.

Audience

Global.

Technical Details

The response code to the authorization says: RC 230: Soft decline. The authorization request was approved by the issuing bank but was flagged because it did not pass the Card Verification Number (CVN) check. You can capture the authorization, but consider reviewing the order for the possibility of fraud.

The error message during capture failure says: Auth code is missing or invalid.

Workaround

None.

Payments | 1576231

Description

A defect is allowing authorizations to succeed when the purchase order number is sent in an incorrect format. These transactions fail during settlement.

Audience

Merchants in the US.

Technical Details

The API field names for the purchase order number field are:

REST API:
orderInformation.invoiceDetails.purchaseOrderNumber
Simple Order API: invoiceHeader_userPO

Workaround

Be sure to send API values using the correct format.

Fraud Management Essentials | 1525926

Description

Due to a defect, when an order that is pending review is viewed in the Transaction Details page in the Business Center, the Marking Tool feature is not available.

Audience

Users of Fraud Management Essentials.

Technical Details

None.

Workaround

Use the Fraud Management Essentials page to review orders until this defect is resolved.

Token Management System (TMS) | 1045848

Description

A defect is affecting TMS in the following scenario:

1. An existing customer token contains an existing payment instrument token that uses either credit card or bank account.
2. An additional payment instrument token is created for that customer token. The first payment instrument token was credit card and the new payment instrument token is bank account, or the old payment instrument token was bank account and the new payment instrument token is credit card.
3. The original payment instrument token is used in an existing autopay.
4. The new payment instrument token is set to default.

The result is that the payment request fails.

Audience

Users of TMS.

Technical Details

None.

Workaround

None.

Decision Manager | 1589720

Description	Merchants that review transactions in Decision Manager are experiencing intermittent timeout failures while searching for customer information in the Negative List.
Audience	Decision Manager users that review customer information in the Negative List.
Technical Details	None.
Workaround	Try selecting a date range to limit the number of results until the defect is fixed.

Payment REST API | 1561824

Description	The Payment REST API is sending HTTP response code 202 instead of 201 when the error reason is contact_processor.
Audience	Users of the Payment REST API.
Technical Details	The affected endpoint is pts/v2/payments.
Workaround	None.

Boarding and Virtual Terminal | 001548638

Description	Virtual Terminal is visible in the Business Center to merchant accounts onboarded to the VAP portfolio that are not enabled for Virtual Terminal.
Audience	Resellers on the VAP portfolio.
Technical Details	None.
Workaround	None.

Reporting | 1542583

Description	A defect is affecting the Transaction Request Report. For some requests that resulted in 102 errors, the Rmsg column is not populated.
Audience	Users of the Transaction Request Report.
Technical Details	None.
Workaround	None.