# Account Comparison Guide

## Reference Information

July 2019

## Authorize.Net Copyright



## Authorize.Net Trademarks



## CyberSource Copyright



## CyberSource Restricted Rights Legends



## CyberSource Trademarks



## CyberSource Contact Information

For general information about our company, products, and services, go to http://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:
http://www.cybersource.com/support

# About This Guide

## Recent Revisions

| Release | Changes |
|---|---|
| June 2019 | First version. |

## Audience and Purpose

This document is for merchants in the UK and European markets who are being upgraded from Authorize.Net to Cybersource to ensure they have support for Strong Customer Authentication as required by the Second Payments Services Directive.

## Related Documentation

Refer to the Support Center for complete CyberSource technical documentation:

http://www.cybersource.com/support_center/support_documentation

# Account Comparison Guide

## Product Support Matrix

Use the following table to find the Cybersource equivalent to the Authorize.Net product or service you use in your business. Click the Authorize.Net product or service listed below for more details, and click the Cybersource equivalent for Cybersource documentation.

| Authorize.Net Product/Service | Cybersource Equivalent Product/Service |
|---|---|
| SIM and Simple Checkout | Secure Acceptance Hosted Checkout |
| DPM | Secure Acceptance Checkout API |
| AIM | REST API |
| Authorize.Net API, XML and SOAP versions | REST API |
| Accept Customer | Secure Acceptance Hosted Checkout, Tokenization Only Option |
| Accept Hosted | Secure Acceptance Hosted Checkout |
| Accept.js | Flex API |
| Accept UI | Flex Microform |
| Accept Mobile | Cybersouce In App SDK for iOS/Android |
| Advanced Fraud Detection Suite | Fraud Management Essentials |
| Customer Profiles | TMS REST API |
| Automated Recurring Billing | Recurring Billing (available date TBD) |
| Invoicing | Cybersource Invoicing (available date TBD) |
| mPOS application | N/A |
| Batch Upload | Batch Transaction Upload |
| Expanded Credit-Return Capabilities | Standalone Credits |
| Sync for QuickBooks/QuickBooks Download | CommerceSync |
| Verified Merchant Seal | N/A |
| Silent Post | Secure Acceptance Transaction POST |
| Webhooks | Webhooks for Cybersource |
| Customer Email Receipts | Secure Acceptance Transaction POST |
| OAuth | OAuth for Cybersource |

# SIM and Simple Checkout

Replacement: Secure Acceptance Hosted Checkout

Secure Acceptance Hosted Checkout enables merchants who don't want to handle or store sensitive payment information to accept payments on a secure checkout page hosted by CyberSource. Using Secure Acceptance Hosted Checkout requires minimal scripting skills. You will also use the Business Center to review and manage orders.

# DPM

Replacement: Secure Acceptance Checkout API

Secure Acceptance Checkout API enables merchants to customize and control their own customer checkout experience, including receipt and response pages. After the customization, you will have full control to store and control customer information before sending it to CyberSource to process transactions, and to use the Business Center to review and manage all of your orders. Using the Secure Acceptance Checkout API requires moderate scripting skills.

# AIM

Replacement: REST API

The Cybersource REST API is a modern API framework that provides access to the full range of Cybersource payments, reporting, fraud management, token management, and user management.Contact your developer partner or solution provider for help in using the REST API in your payment flow.

# Authorize.Net API, XML and SOAP versions

Replacement: REST API

The Cybersource REST API is a modern API framework that provides access to the full range of Cybersource payments, reporting, fraud management, token management, and user management.Contact your developer partner or solution provider for help in using the REST API in your payment flow.

# Accept Customer

Replacement: Secure Acceptance Hosted Checkout, Tokenization Only Option

Secure Acceptance Hosted Checkout enables merchants who don't want to handle or store sensitive payment information to accept payments on a secure checkout page hosted by CyberSource. After enabling payment tokenization for Secure Acceptance, you can create and retrieve payment tokens through the Token Management Service.

Using Secure Acceptance Hosted Checkout requires minimal scripting skills. You will also use the Business Center to review and manage orders.

# Accept Hosted

Replacement: Secure Acceptance Hosted Checkout

Secure Acceptance Hosted Checkout enables merchants who don't want to handle or store sensitive payment information to accept payments on a secure checkout page hosted by CyberSource. Using Secure Acceptance Hosted Checkout requires minimal scripting skills. You will also use the Business Center to review and manage orders.

# Accept.js

Replacement: Flex API

Flex API is suitable for use cases that require access to customer's payment information in client-side code.

For example, you can use this API to detect gift cards and route them differently. You can also use the Flex API for implementation into applications. Using this API can qualify you for PCI DSS assessments based on SAQ A-EP.

# Accept UI

Replacement: Flex Microform

Flex Microform is a CyberSource-hosted page that replaces the card number input field and calls the Flex API on your behalf. You can style this page to look like and behave the same as any other field on your website.

Flex Microform provides the most secure method for tokenizing card data. Sensitive data is encrypted on the customer's device before HTTPS transmission to CyberSource. This method mitigates any compromise of the HTTPS connection by a man-in-the-middle attack.

# Accept Mobile

Replacement: Cybersouce In App SDK, iOS and Android versions

The Cybersource In App SDK provides simple functionality to dispatch sensitive credit card data directly to CyberSource, returning a safe payment token that can be passed up to your mobile backend for standard CyberSource processing without the burden of credit card data reaching your server. With the secure payment token, your server can create a CyberSource subscription, long term token or payment.

# Advanced Fraud Detection Suite

Replacement: Fraud Management Essentials (requires EBC login to view documentation)

Decision Manager gives you the ability to customize rules and models to your specific business, across all sales channels, including web, mobile, call center, and kiosks. Along with a flexible rule engine, Decision Manager helps you optimize your fraud processes through Real-Time Fusion Modeling technology that blends multiple advanced machine learning methods for accurate scoring.

# Customer Profiles

Replacement: TMS REST API

The CyberSource Token Management Service (TMS) enables you to safely store customer information, including payment data, in secure Visa data centers. It replaces this data with tokens in requests to other CyberSource services.

To learn more about CyberSource REST APIs, see Getting Started with the CyberSource REST API.

# Automated Recurring Billing

Replacement: Recurring Billing (available date TBD)

# Invoicing

Replacement: CyberSource Invoicing (available date TBD)

# Batch Upload

Replacement: Batch Transaction Upload

Batch Upload uses Offline Transaction File Submission to send CyberSource a single file, called a batch file or batch transaction file, that contains a set (batch) of transaction requests instead of sending individual requests for each transaction. The information you provide for each request in the batch file is the same information you provide for an individual service request.

# Expanded Credit-Return Capabilities

Replacement: Standalone Credits

Standalone credits are enabled for CyberSource merchants by default.

# Verified Merchant Seal

Replacement: N/A

The Verified Merchant Seal is deprecated and will not be replaced.

# Silent Post

Replacement: Secure Acceptance Transaction POST

Secure Acceptance Hosted Checkout enables merchants who don't want to handle or store sensitive payment information to accept payments on a secure checkout page hosted by CyberSource. Using Secure Acceptance Hosted Checkout requires minimal scripting skills. You will also use the Business Center to review and manage orders.

CyberSource recommends implementing the merchant POST URL notification as a backup means of determining the transaction result. This method does not rely on your customer’s browser. You receive the transaction result even if your customer lost connection after confirming the payment.

# Webhooks

Replacement: Webhooks for Cybersource

Webhooks for CyberSource is currently under development and should be available on or shortly after September 14, 2019. CyberSource recommends that you integrate your payment solution to use 3DS for Strong Customer Authentication prior to implementing webhooks.

# Customer Email Receipts

Replacement: Secure Acceptance Transaction POST

Secure Acceptance Hosted Checkout enables merchants who don't want to handle or store sensitive payment information to accept payments on a secure checkout page hosted by CyberSource. Using Secure Acceptance Hosted Checkout requires minimal scripting skills. You will also use the Business Center to review and manage orders.

You can send a purchase receipt email to your customer and a copy to your own email address. Both are optional. Customers can reply with questions regarding their purchases, so use an active email account. The email format is HTML unless your customer email is rich text format (RTF).

# OAuth

Replacement: OAuth for Cybersource

OAuth for CyberSource is currently under development and should be available on or shortly after September 14, 2019. CyberSource recommends that you integrate your payment solution to use 3DS for Strong Customer Authentication prior to implementing OAuth.