Cybersource Product Note

May 2026

cybersource
A Visa Solution

Version: 2

Contents

Product Note

Welcome to the Product Note for May 2026.

The Product Note provides information about product enhancements and updates to key initiatives that were released to production in May 2026. It also highlights product enhancements and updates that are planned for future releases.

Product and Feature Development Stages

A product or feature goes through several stages of development during the federal fiscal year (FY):

Table 1. Product and Feature Development Stages

Stage	Definition
IN DEVELOPMENT	The product or feature is in development, which could take 90 or more days to reach the release candidate stage.
RELEASE CANDIDATE	The product or feature is ready to enter the release cycle and is approximately 30 days from entering the release pending stage.
RELEASE PENDING	The product or feature is scheduled for release to production.
RELEASED	The product or feature is released and in production.

Related Information

Visit the Documentation hub on the Cybersource Developer Center for these documents:

- **Release Notes:** include information about feature enhancements and bug fixes released each week.
- **Product documentation:** includes implementation, developer, and user guides for Cybersource products.

Announcements

These announcements apply to May 2026.

Bluefin P2PE Decryption: PCI P2PE Support Ending for PTS 3.X Terminals

Bluefin announced that their support for PCI P2PE on PTS 3.X payment terminals ended on **April 30, 2026**. These devices are no longer supported or listed as part of Bluefin's validated PCI P2PE solution.

Bluefin notified clients about the device support status. Customers still using PTS 3.X devices should transition to supported alternatives to remain compliant. For replacement and integration guidance, see the Guidance on Expiring Bluefin P2PE PTS Devices document.

Message-Level Encryption Upcoming Mandate

An updated version of message-level encryption (MLE) will become mandatory so that merchants can use Cybersource APIs. Portfolio owners must enable this updated version of MLE for their merchants by **September 2026**.

This required MLE update encrypts all data in your API response messages. The previous version of MLE encrypted only request messages. If your merchants are already using custom JSON Web Token (JWT) messaging, they must also update how their system constructs JWTs. For merchants who are using HTTP signature messaging, they must migrate their system to JWT messaging.

Warning:

You risk transaction failures if you do not implement this MLE update.

Overview of MLE

MLE is a robust security protocol designed to encrypt individual messages or payloads at the application layer. By protecting sensitive data at the message level, MLE ensures that your information remains secure as it moves across systems and networks, providing a layer of security beyond traditional transport encryption.

Enabling MLE requires you to create a REST API key for request messages and a *REST – API Response MLE* key for response messages. If your organization is using a meta key, the portfolio account or merchant account user who created the meta key must also create the REST – API Response MLE key.

Update Methods

- Create or update your custom MLE integration using JWTs with P12 certificates. For more information, see the Enable Message-Level Encryption section in the *Getting Started with REST Developer Guide*. For a method using shared secret key pairs, see *HTTP Messaging Migration to JWT Messaging* below.
- Update your REST API SDK. For more information, see the *REST API related products* section in the Cybersource GitHub.

JSON Web Token Construction Update

These actions are now required so that API requests can be sent to Cybersource. If you use a custom integration to construct JWTs, you must update your system to remain compliant. This update is necessary to support the new MLE requirements.

Update Methods

- See Construct JWT Messages Using a P12 Certificate in the *Getting Started with REST Guide*
- See Construct JWT Messages Using a Shared Secret Key Pair in the *Getting Started with REST Guide*

HTTP Messaging Migration to JWT Messaging

By **September 2026**, all merchants using HTTP signature messaging must migrate to JWT messaging in order to support MLE. Merchants already using HTTP signature messaging with shared secret key pairs can continue using their existing keys with JWT messaging.

Update Method

See Construct JWT Messages Using a Shared Secret Key Pair in the *Getting Started with REST Guide*

Smart Auth Retirement

Smart Auth, also known as SuperAuth, is being discontinued. This product was often included in the essentials package of products for small businesses.

Support for Smart Auth is being discontinued in phased approaches. End of life will occur October 5, 2026.

Important: Merchants currently using Smart Auth will receive a 90-day product sunset notification.

Merchants interested in a similar product can use Fraud Management Essentials (FME). FME is an actively supported service that offers improved fraud protection capabilities and system reliability.

TLS Updates

We are making changes to our implementation of Transport Layer Security (TLS).

TLS 1.3

To maintain the highest security standards for both browser-based and server-to-server connections, we will enable TLS 1.3 on the endpoints listed below. This enhancement is optional and will supplement the existing TLS 1.2 support, which will remain in place.

We will make changes to these endpoints on these dates:

Production environment: June 9, 2026

ics2wsa.ic3.com

ics2ws.ic3.com

api.cybersource.com

The test versions of of these environments have already been updated.

Contact Customer Support if you have any questions about these changes.

TLS Certificate Lifetime Reduction

In alignment with new CA/Browser Forum regulations, the maximum TLS certificate lifetime will be reduced gradually as follows:

• Currently, the maximum lifetime for a TLS certificate is 200 days.

• Beginning March 15, 2027, the maximum lifetime for a TLS certificate will be 100 days.

• Beginning March 15, 2029, the maximum lifetime for a TLS certificate will be 47 days.

See this blog for more information about the TLS certificate lifetime changes:

https://www.digicert.com/blog/tls-certificate-lifetimes-will-officially-reduce-to-47-days

How will this change impact connectivity?

Server-level (leaf) SSL/TLS certificates will remain valid until their scheduled expiration. Server-level (leaf) TLS certificates have shorter lifespans and must be reissued more frequently. We therefore recommend that clients trust the root certificate instead.

What is our recommendation?

We continue to recommend trusting the Root TLS certificates for all secure endpoints. This approach removes the need for periodic renewal of server level certificates and helps prevent connection failures caused by expired leaf certificates.

How can I tell which TLS certificate I am using?

Contact your server administrator or your network support team.

Where can I find the TLS Root certificate?

Continue trusting the root certificate to maintain connectivity with supported endpoints. You can download the root certificate from this article:

https://support.visaacceptance.com/knowledgebase/Knowledgearticle/?code=KA-09802

Contact your Customer Support representatives with any questions.

Webhooks Updates

Webhooks version 1 will be decommissioned by end of the year 2026. See Webhooks version 2 in the Developer Center.

Enhanced Webhook URL Review and Approval Process

We are introducing an enhancement to webhook subscription processing to improve security, compliance, and visibility for webhook-related URLs. Webhook URLs will be validated and reviewed before they can be used. This includes both newly submitted subscriptions and existing subscriptions currently on file. This change is expected to take place in June 2026.

What is Changing

When a webhook subscription is created or updated, the URLs associated with that subscription will be evaluated through a validation and approval process.

This applies to:

- **Webhook URL** (required)
- **OAuth URL** (if applicable)
- **Health Check URL** (if applicable)

As part of this enhancement, clients might now see the following user-facing statuses:

- **PENDING_REVIEW**
- **BLOCKED**

The existing **INACTIVE** status remains unchanged and continues to indicate that the subscription is approved and ready within the current lifecycle.

Status Descriptions

Status	Description
PENDING_REVIEW	One or more submitted URLs are being validated or awaiting required security approval.
BLOCKED	One or more URLs were rejected or identified as unsafe or non-compliant. The subscription cannot proceed until the URL(s) are updated.
INACTIVE	All required approvals are complete, and the subscription is ready under the existing activation flow.

How the New Process Works

1. A webhook subscription is created or updated.
2. Submitted URLs are checked against existing approval records.
3. New or unknown URLs are evaluated through automated validation.
4. If additional review is required, the subscription status changes to **PENDING_REVIEW**.
5. If any URL is rejected or blocked, the subscription status changes to **BLOCKED**.
6. If all required URLs are approved, the subscription status changes to **INACTIVE**.

Impact on Existing Subscriptions

After this change goes live, we will run existing webhook subscriptions through the new validation process:

- Existing subscription URLs will be assessed using the new validation framework.
- URLs that require additional security review might change the status of the subscription to **PENDING_REVIEW**.
- If any existing URL is identified as blocked, the associated subscription status will be updated to **BLOCKED**.

In cases where a subscription status is change to **BLOCKED**, clients will be expected to perform these tasks:

- Review the affected endpoint(s).
- Update the URL(s) to an acceptable endpoint.
- Resubmit the subscription for processing.

For New Subscriptions

New webhook-related URLs may go through validation and, if necessary, security review before the subscription can proceed.

For Existing Subscriptions

Current subscriptions will also be reviewed after they go live. If an existing endpoint does not meet the new validation requirements, the subscription status might be updated to **BLOCKED** until the URL is corrected.

If Your Subscription Is Marked BLOCKED

This means one or more URLs associated with the subscription cannot be used in their current form. To continue, the client must update the affected URL(s) and resubmit.

Why We Are Making This Change

This enhancement is designed to:

- **Reduce security risk** by preventing outbound calls to unapproved endpoints.
- **Improve compliance** through stronger review and approval controls.
- **Increase transparency** with clearer client-visible statuses.
- **Support scale** through a standardized and repeatable validation process.

Features Released in May 2026

This section provides information about product enhancements and updates to key initiatives that were released to production in May 2026.

New Unified Checkout SDK Components Function to Enable Header Bar Removal in Unified Checkout

Products Included: Unified Checkout and Click to Pay Drop-In UI

Region/Country: Global

Release Date: RELEASED | May 2026

Internal Feature Number: 203478

Mandate: Does not apply

Description

This enhancement allows for embedded elements of the card capture/ Click to Pay payment process to be embedded into a merchant's payment page. By using the components feature, the header for Unified Checkoutdoes not appear and only the payments UI is rendered.

Merchant Impact

There is no impact to existing integrations. Merchants that want to integrate using the components feature can use this new SDK function in their integration

Benefit

This release creates an embedded experience for merchants without the need to use the Unified Checkout Manual Card Entry / Click to Pay payment button. This enables merchants to embed only the payments UI on their payment page.

Expand Unified Checkout Local Market Relevance

Products Included: Unified Checkout and Click to Pay Drop-In UI

Region/Country: AP, CEMEA, EU, LAC, NA

Release Date: RELEASED | May 2026

Internal Feature Number: 21123

Mandate: Does not apply

Description

This release expands Unified Checkout and Click to Pay localization elements to support global markets. Enhancements include right-to-left language support for Arabic languages and additional locales for LAC and CEMEA.

These locales are now supported:

- ar_JO
- ar_QA
- en_AE
- en_QA

Merchant Impact

Merchants can expand into Arabic-speaking markets with right-to-left language support.

Benefit

Localization expands market reach, improves conversion rates, and positions Unified Checkout and Click to Pay as the go-to solutions for global merchants.

This release expands localization of Unified Checkout and Click to Pay flows for Arabic-speaking customers.

Visa Payment Passkey Authentication via Unified Checkout

Products Included: Unified Checkout

Region/Country: AP, CEMEA, EU, LAC, NA

Release Date: RELEASED | May 2026

Internal Feature Number: 217527

Mandate: Does not apply

Description

This enhancement enables users that are using Payer Authentication via Unified Checkout to use Visa Payment Passkey for authentication in place of traditional 3-D Secure experiences.

This release supports the following consumer journeys:

- Consumers not yet enrolled in Visa Passkey can enroll during the Payer Authentication validation flow.
- Consumers already enrolled in Visa Passkey can use Passkey authentication as a replacement for the issuer-hosted 3-D Secure challenge.

Passkey authentication applies to Visa cards only and requires Payer Authentication to be enabled for the merchant.

Merchant Impact

This change applies to merchants and resellers using Unified Checkout with Payer Authentication enabled. Merchants can request Passkey authentication for their Payer Authentication journey by specifying `PASSKEY` as the `consumerAuthenticationType` in the Complete API request.

If Passkey is not available, the authentication flow defaults to traditional 3-D Secure experiences.

Merchants that do not use 3-D Secure Payer Authentication are not impacted. No integration changes are required to receive the updated iframe-compatible behavior.

Merchants must reach out to their representative for Passkey to be enabled for their Payer Authentication configuration.

Benefit

Benefits include higher authentication success rates, reduced consumer abandonment, and a simplified integration path for Passkey-based authentication, advancing Visa's strategy for secure and seamless checkout through Unified Checkout.

Regional Wallet Support for Unified Checkout

Products Included: Unified Checkout

Region/Country: CEMEA, EU, AP, and NA

Release Date: RELEASED | May 2026

Internal Feature Number: 25525

Mandate: Does not apply

Description

This release expands regional network support for digital wallets and direct wallet integrations for Unified Checkout. Your integration can now support these domestic card schemes through Apple Pay:

- Cartes Bancaires
- Jaywan
- mada
- Meeza

Merchant Impact

Merchants can accept widely used domestic card schemes through Apple Pay and Unified Checkout without building market-specific integrations. Merchants can meet regulatory mandates, expand wallet acceptance, and improve conversion rates in key regions.

Benefit

By extending wallet support across regional networks, Unified Checkout strengthens global adoption, accelerates wallet usage, and ensures that merchants can serve local customers.

REST Client SDK Update for Java and .NET

Products Included: REST Client SDK

Region/Country: All

Release Date: RELEASED | May 2026

Internal Feature Number: 193763

Mandate: Does not apply.

Description

The REST Client SDK is updated to support the new JSON Web Token (JWT) message construction and Message-Level Encryption (MLE) enablement requirements for the Java and .NET programming languages.

Additional languages will be supported in a future update. For more information, see REST Client SDK Update for Node, PHP, Python, and Ruby (on page 51).

Warning:

To avoid potential transaction failures, portfolio owners must enable this updated version of MLE for their merchants by **September 2026**.

Benefit

The REST Client SDK provides merchants with an alternative method to integrating to Cybersource REST APIs. This method enables merchants to send and receive REST API messages using REST Client SDK instead of creating a custom set up.

The updated SDK also keeps merchants in compliance with the new JWT-based message construction and updated MLE requirements.

Merchant Impact

Merchants already using the REST Client SDK should update to the newest SDK version to remain in compliance.

Warning: You risk transaction failures if you do not update your system to support the new JSON Web Token (JWT) message construction and Message-Level Encryption (MLE) enablement requirements.

Paze Support for Discover

Products Included: Paze

Region/Country: NA

Release Date: RELEASED | May 2026

Internal Feature Number: 34285

Mandate: Does not apply

Description

Paze now supports the Discover card network. Discover cards can be provisioned, tokenized, stored, and transacted in Paze with full lifecycle management, consistent with existing supported card networks. Support is available across both direct Paze integrations and Unified Commerce implementations, ensuring a consistent checkout experience for merchants and consumers. This update requires no changes to existing merchant integrations and maintains parity with current wallet functionality.

Merchant Impact

No changes are required to existing merchant integrations. Merchants automatically gain support for Discover transactions when the feature is available and properly configured. Standard transaction processing, reporting, and reconciliation workflows remain unchanged. Merchants should validate Discover transactions in test environments as soon as issuer and network certifications are complete.

Benefit

- **Expanded Customer Reach:** Accepts transactions from Discover cardholders.
- **Increased Conversion Opportunities:** Reduces checkout friction by supporting more eligible wallet users.
- **Higher Transaction Volume:** Increases use of Paze across existing merchant flows.
- **Consistent Checkout Experience:** Maintains a unified payment experience across card networks.

Expanded Regional Support for Tink Pay By Bank

Products Included: Unified Checkout

Region/Country: AP, CEMEA, EU, LAC, NA

Release Date: RELEASED | May 2026

Internal Feature Number: 201670

Mandate: Does not apply

Description

Unified Checkout expands its Tink integration to support additional European markets, including France, Germany, Ireland, Spain, and the Netherlands.

This enhancement enables merchants to offer open banking payment methods through a unified integration, using a redirect-based flow with transaction status validation consistent with existing Tink implementations.

Merchant Impact

Merchants can accept open banking payments across additional European markets without building separate, country-specific integrations.

These enhancements enable merchants to:

- Expand into key EU markets using a single Unified Checkout integration.
- Offer consumer-preferred open banking payment methods.
- Reduce integration complexity through a unified payment experience.
- Access new revenue opportunities tied to alternative payment methods.

Benefit

By expanding Tink-supported markets, Unified Checkout lowers the barrier to adopting open banking payments and enables merchants to scale more efficiently across Europe.

These enhancements support global expansion strategies, increase adoption of alternative payment methods, and improve checkout conversion by aligning with regional payment preferences.

Tink Pay by Bank Now Offered in Europe

Products Included: Tink by Bank

Region: Europe

Release Date: RELEASED | May 2026

Internal Feature Number: 201670

Description

Tink Pay by Bank accepts payments using the euro in these countries:

- France
- Germany
- Ireland
- Netherlands
- Spain

Merchant Impact

Merchants who want to process payments in the listed countries using Tink Pay by Bank can now integrate, or update their existing integration, to the Cybersource API. For more information, see the *Tink Pay by Bank Developer Guide*.

Benefit

This update enables merchants in the listed European markets to begin processing payments using Tink Pay by Bank.

Mastercard Click to Pay Enhancements

Products Included: Unified Checkout, Click to Pay Drop-In UI, and Unified Click to Pay

Region/Country: Global; Brazil (LAC features)

Release Date: RELEASED | May 2026

Internal Feature Number: 28169

Mandate: Does not apply

Description

This release delivers a set of enhancements to the Mastercard Click to Pay experience within Unified Checkout, Unified Click to Pay, and Click to Pay Drop-In UI, bringing parity with the Visa Click to Pay integration across authentication, checkout flow, and regional support.

Mastercard Authentication

Mastercard will handle authentication within the Click to Pay customer experience using the optimal method based on device, amount, and region. This includes in-app authentication, biometrics, 3-D Secure, CVV step-up, and Mastercard Payment Passkeys. Authentication outcomes are returned in the transient token and Get Payment Credentials API response.

Mastercard Loading Digital Commerce Framework (DCF)

The Mastercard DCF will now act as a loading DCF, not requiring a consumer to interact and enter additional information within the checkout flow. Customers complete all steps, including billing and shipping details, card linking, and Remember Me selection, within Unified Checkout, Unified Click to Pay, or Click to Pay Drop-In UI without having to re-enter information in a separate Mastercard window.

Merchant Impact

Merchants using Mastercard Click to Pay via Unified Checkout, Unified Click to Pay, or Click to Pay Drop-In UI will benefit from improved authentication rates and a streamlined checkout experience without DCF redirect. Authentication results are available in the API response for all transactions. No integration changes are required in order to receive the updated authentication and DCF behavior for merchants that are using Unified Checkout or Click to Pay Drop-In UI version 1 or higher.

Benefit

These enhancements bring full parity between Visa and Mastercard within the Click to Pay experience, providing a consistent, scheme-agnostic checkout across both networks. Merchants benefit from higher authentication success rates, reduced consumer abandonment, and elimination of the DCF redirect—keeping consumers within a single, cohesive payment flow.

Payer Interface Upcoming Features

This section provides information about payer interface product enhancements and updates that are planned for future releases.

Audit Logging for Invoicing

Products Included: Invoicing

Region/Country: Global

Release Date: IN DEVELOPMENT | Q4 FY26

Internal Feature Number: 13331

Description

The Audit Search feature of the Business Center will show audit logs for creating and modifying invoices and their settings. To view the audit logs, go to **Tools > Audit Search**.

Merchant Impact

Merchants and resellers will be able to search audit logs for actions performed in a merchant's account and determine who performed those actions. Resellers and merchants will know which actions were performed by support staff on behalf of the merchant.

Expiration Date Based on Volume and Count for Pay by Link

Products Included: Pay by Link

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | Q4 FY26

Internal Feature Number: 95249

Mandate: Does not apply

Description

This enhancement provides merchants with additional criteria for an expiring payment link:

- A transaction amount limit for a customer-set price link
- A transaction count limit for a fixed-price link

When the defined expiration amount or quantity is reached, the link expires and payers can no longer make a payment.

Important: if a payer initiates a higher quantity or amount transaction before the limit is reached, the defined quantity or amount expiration limit might be slightly exceeded.

Merchant Impact

- **When creating a customer-set price payment link:** In addition to setting the expiration date, merchants can set a transaction amount above which the payment link will expire. One or both expiration criteria can be set. If both expiration criteria are set, whichever criterion is met first causes the link to expire.

- **When creating a fixed price payment link:** In addition to setting the expiration date, merchants can set an expiration quantity above which the payment link will expire. One or both expiration criteria can be set. If both expiration criteria are set, whichever criterion is met first causes the link to expire.

Benefit

A merchant can automatically stop accepting payments on a link when their target amount is reached (such as a donation target or a campaign target).

The transaction count limit can indicate the available inventory. A merchant can automatically stop accepting payment on a link when the limit of their available inventory is reached.

Enhanced Notification Design for Invoicing and Pay by Link

Products Included: Invoicing and Pay by Link

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | Q4 FY26

Internal Feature Number: 205140

Description

Invoicing and Pay by Link is introducing a branded, mobile-friendly design for invoicing and Pay by Link email notifications for merchants and partners. Changes to email notifications includes:

- Updated notifications and receipts for Invoicing and Pay by Link
- Support for merchant and partner branding
- Consistent visuals and tone
- Mobile-first, professional design in line with Visa standards

Merchant Impact

No action is required by merchants. The logo, address, phone number, website, and tax number added to the Business Center automatically appears in the email notification.

Partner Impact

No action is required by partners. The partner's default brand portfolio logo is automatically used in the email footer. Partners with branded portfolios can co-brand emails or offer merchants the option to use their logo.

Merchant Brand Settings for Invoicing and Pay by Link

Products Included: Pay by Link and Invoicing

Region/Country: Global

Expected Release Date: RELEASE CANDIDATE | June 2026

Internal Feature Number: 189468

Mandate: Does not apply

Description

Invoicing and Pay by Link leverage Unified Checkout merchant settings. Merchants can customize the look and feel of their payment pages, manage payment methods, and collect required information from their payers in the checkout flow.

Merchant Impact

To configure Unified Checkout merchant settings, go to the Business Center and follow these steps:

1. Navigate to **Payment Configuration > Unified Checkout**.
2. Click **Manage** for the category you want to update.
3. Make the desired changes.
4. Click **Save and publish**.

Benefit

Merchants can customize the appearance of their payment pages, manage payment methods, and collect required information from their payers in the checkout flow.

Merchants can choose either authorization or sale (authorization and capture) for invoicing and Pay by Link payments. To access these settings, go to the left navigation panel and choose **Payment Configuration > Unified Checkout**.

Support for New Payment Methods for Invoicing and Pay by Link

Products Included: Invoicing and Pay by Link

Region/Country: Global

Expected Release Date: RELEASE CANDIDATE | June 2026

Internal Feature Number: 122459

Description

To help merchants offer their clients flexible payment options and speed up checkout, Invoicing and Pay by Link now support new payment methods and card types through Unified Checkout.

New payment methods and card types include:

- iDEAL: Netherlands
- Multibanco: Portugal
- Przelewy24: Poland
- MyBank: Belgium
- Dragon Pay: Philippines
- Bancontact: Belgium
- Tink (Pay by Bank): United Kingdom
- Jaywan: UAE
- UATP: US and Europe
- KCP: Korea

Merchant Impact

Merchants can enable these payment methods through their reseller or customer support.

Regional Wallet Support for eftpos on Unified Checkout

Products Included: Unified Checkout

Region/Country: CEMEA, EU, AP, and NA

Expected Release Date: RELEASE CANDIDATE | Q1 FY27

Internal Feature Number: 25525

Mandate: Does not apply

Description

Regional network support for digital wallets expands Unified Checkout and direct wallet integrations to support eftpos through Apple Pay.

Merchant Impact

Merchants can accept widely used domestic card schemes through Apple Pay and Unified Checkout without building market-specific integrations. Merchants can meet regulatory mandates, expand wallet acceptance, and improve conversion rates in key regions where domestic networks drive consumer preference.

Benefit

With wallet support across regional networks, Unified Checkout strengthens global adoption,accelerates wallet usage, and ensures that merchants can serve local customers

Remove Contact Details Step from Click to Pay in Unified Checkout

Products Included: Unified Checkout

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 203561

Mandate: Does not apply

Description

This update removes the Contact Details section from the Unified Checkout checkout UI for Click to Pay implementations when `requestEmail=false` and `requestPhone=false` are configured in the Capture Context. When neither email nor phone collection is required, the Contact Details section will no longer appear in the payment UI when the customer email address is included in the Sessions API request.

The Contact Details section was originally included to support Click to Pay customer lookup flows. When merchants did not require contact data collection, the section became redundant and caused the Click to Pay email address to appear in two places within the UI, once in the Contact Details section and again in the Payment Details tab. This created duplication and confusion for customers. This change ensures the checkout UI reflects the merchant's capture mandate configuration.

Merchant Impact

This change applies to merchants using Click to Pay within Unified Checkout where `requestEmail=false` and `requestPhone=false` are set in the Capture Context. No integration changes are required. The Contact Details section will be automatically omitted from the checkout UI when contact data collection is not requested and the email address is provided in the **data.orderInformation.billTo.email** field in the Sessions API request.

Merchants that require email or phone collection are not affected, and the Contact Details section will continue to appear as expected for those configurations.

Benefit

By removing the Contact Details step when contact data is not required, this release reduces checkout friction and eliminates duplicate information display in the Click to Pay flow. The checkout experience now accurately reflects each merchant's capture mandate, providing consumers with a simpler, more consistent payment presentation.

Payment Processing Upcoming Features

This section provides information about payment processing product enhancements and updates that are planned for future releases.

Account Name Inquiry for FDC Nashville Global

Products Included: Authorizations, zero-amount authorizations for account verification, account funding transactions (AFTs), and original credit transactions (OCTs)

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 28438

Mandate: Does not apply

Description

Account name inquiry (ANI) verifies that the cardholder's name matches the name on their issuer bank account. You must request ANI during a zero-amount authorization before payment authorizations or full financial transactions, including account funding transactions (AFTs) and original credit transactions (OCTs). Initiate an ANI during customer account setup, periodically, or on demand. Use the match results to decide whether to proceed, retry, or flag for fraud checks. Pre-transaction ANI verification reduces fraud risk, especially in AFT and OCT transactions.

ANI is automatically enabled for your account and available for Mastercard and Visa cards.

Merchant Impact

Request the service by sending the following fields with the cardholder's name on the zero-amount authorization request:

- REST API: **processingInformation.cardVerification.checkANI** Set to `Y`.
- Simple Order API: **businessRules_checkANI** Set to `Y`.

You can specify the name match results (full, partial, or no match) to tell the system to decline the transaction.

Benefit

ANI helps you decide whether to proceed, retry, or flag the account for a fraud review.

Account Name Inquiry for Barclays

Products Included: Payment Processing

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 9228

Mandate: Does not apply

Description

Account name inquiry (ANI) verifies that the cardholder's name matches the name on their issuer bank account. You must request ANI during a zero-amount authorization before payment authorizations or full financial transactions, including account funding transactions (AFTs) and original credit transactions (OCTs). Initiate an ANI during customer account setup, periodically, or on demand. Use the match results to decide whether to proceed, retry, or flag for fraud checks. Pre-transaction ANI verification reduces fraud risk, especially in AFT and OCT transactions.

ANI is automatically enabled for your account and available for Mastercard and Visa cards.

Merchant Impact

Request the service by sending the following fields with the cardholder's name on the zero-amount authorization request:

- REST API: **processingInformation.cardVerification.checkANI** Set to `Y`.
- Simple Order API: **businessRules_checkANI** Set to `Y`.

You can specify the name match results (full, partial, or no match) to tell the system to decline the transaction.

Benefit

ANI helps you decide whether to proceed, retry, or flag the account for a fraud review.

Account Name Inquiry for GSAPv3

Products Included: Payment Processing

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Numbers: 33555 & 209043

Mandate: Does not apply

Description

Account name inquiry (ANI) verifies that the cardholder's name matches the name on their issuer bank account. You must request ANI during a zero-amount authorization before payment authorizations or full financial transactions, including account funding transactions (AFTs) and original credit transactions (OCTs). Initiate an ANI during customer account setup, periodically, or on demand. Use the match results to decide whether to proceed, retry, or flag for fraud checks. Pre-transaction ANI verification reduces fraud risk, especially in AFT and OCT transactions.

ANI is automatically enabled for your account and available for Mastercard and Visa cards.

Merchant Impact

Request the service by sending the following fields with the cardholder's name on the zero-amount authorization request:

- REST API: **processingInformation.cardVerification.checkANI** Set to `Y`.
- Simple Order API: **businessRules_checkANI** Set to `Y`.

You can specify the name match results (full, partial, or no match) to tell the system to decline the transaction.

Benefit

ANI helps you decide whether to proceed, retry, or flag the account for a fraud review.

Batch Upload API Key for Offline Transaction File Submissions

Products Included: Offline Transaction File Submission

Country/Region: Global

Release Date: June 2026

Description

You can now create a batch upload API key in the Business Center in order to submit an offline transaction file. A batch upload API key is required for offline transaction file submissions.

Merchant Impact

Merchants can create their own batch upload API key using their Business Center account.

Benefit

Merchants no longer have to contact customer support to receive a batch upload key. This new feature enables merchants to begin submitting offline transaction files faster.

Capture Status for Authorize and Capture Transactions to be Fixed

Products Included: Payments

Region/Country: Global

Expected Release Date: RELEASE CANDIDATE | June 2026

Internal Feature Number: 211858

Mandate: Does not apply

Description

Authorize and Capture (bundled) transactions processed through GPN using the Payments 2.0 API are returning PENDING status instead of AUTHORIZED. This will be fixed in early June.

Merchant Impact

The status will display correctly, and in accordance with the API documentation.

Benefit

This update will eliminate confusion about the status of these transactions.

Digital Wallets for Prosa

Products Included: Apple Pay and Google Pay

Region/Country: Mexico

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 215292

Mandate: Does not apply.

Description

This release adds full support for digital wallet transactions on the Prosa gateway, including Apple Pay and Google Pay, for authorization and follow-on transactions. The enhancement implements network token processing to correctly transmit network token cryptograms for Visa and Mastercard transactions.

Merchant Impact

Merchants will be able to enable Apple Pay and Google Pay on the gateway and process digital wallet transactions for both Visa and Mastercard with improved acceptance. For Mastercard PAN-only Google Pay transactions, payer authentication may return an `unavailable` status, however, the authorization might still be approved, and no merchant action will be required. This enhancement will enable consistent digital wallet processing and resolve ongoing issues with the service.

Benefits

- Enables reliable processing of Apple Pay and Google Pay transactions on Prosa.
- Improves authorization success rates for Visa and Mastercard digital wallet transactions.
- Ensures correct transport of network token cryptograms across all applicable transaction types.
- Removes uncertainty around digital wallet support on the Prosa gateway.

Installment Plan Simplification for Cielo

Products Included: Payments processing

Region/Country: Brazil

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 28055

Mandate: Does not apply

Description

The Cielo Installment Simplification feature standardizes how installment plan information is sent and processed for transactions routed through Cielo. The enhancement simplifies installment data handling by allowing merchants to send normalized installment values while maintaining compatibility with Cielo and network requirements.

Merchant Impact

Merchants processing installment transactions through Cielo must ensure their systems are updated to send simplified installment values as supported by this enhancement. Existing installment functionality continues to be supported, with simplified handling improving overall processing consistency.

Benefits

- Simplifies installment configuration for merchants processing through Cielo
- Reduces complexity and variation in installment plan data
- Improves consistency and reliability of installment transaction processing
- Supports cleaner data handling across authorization and settlement flows

Mastercard Transaction Link Identifier

Products Included: Payment Processing

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 3003177

Mandate: AN 7102 Mastercard Transaction Link Identifier (TLID)

Description

The Mastercard Transaction Link Identifier (TLID) is a unique transaction identifier generated by Mastercard. The advanced design of TLID improves the current identifiers and helps ensure a consistent transaction identification methodology between the Mastercard network and its customers. It also provides a means to track a transaction across multiple stages over time.

Merchant Impact

Merchants will see the TLID returned in all authorization, authorization reversal, and credit authorization responses in these fields:

- REST: **processorInformation.transactionLinkIdentifie**
- Simple Order: **paymentNetworkTransactionLinkIdentifier**

These TLID fields that were released for Visa Platform Connect will be deprecated:

- REST: **issuerInformation.transactionInformation**
- REST: **processorInformation.lifecycleTransactionId**
- Simple Order: **paymentNetworkTransactionLinkIdentifier**
- Simple Order: **lifecycle_transactionId**

Benefits

- Globally unique transaction identification.
- Consistency and alignment across all acceptance brands and message specifications, regardless of the Mastercard platform on which they originated.
- Matching and linking all messages across the entire lifecycle of a transaction.
- Improved ability to detect unauthorized or fraudulent activity.
- Improved quality and simplification of operational research processes.

Merchant Country of Origin for TSYS Acquiring Solutions

Products Included: Payment Processing

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Numbers: 208110 & 34076

Mandate: Does not apply

Description

This feature will add support for merchant country of origin in authorization requests on TSYS Acquiring Solutions. This field identifies the country where a merchant is legally registered. It is required for government-controlled entities where the country of origin differs from the merchant country.

Merchant Impact

Government-controlled merchants must include merchant country of origin in authorization requests when the country of origin differs from the merchant country. This measure ensures the Mastercard compliance threshold of 99.9%.

Benefit

Support for merchant country of origin support ensures compliance with Mastercard requirements, avoiding non-compliance fines for government entities.

Merchant-Initiated Partial Authorization Reversals for GSAPv3

Products Included: Payment Processing

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Numbers: 33557 & 209051

Mandate: Does not apply

Description

This release enables merchants to partially reverse authorizations on GSAPv3. Partial authorization reversals release unused holds when final charges are lower than initial estimates. It is commonly used in hotels, fuel stations, and e-commerce.

Merchant Impact

Merchants can partially reverse uncaptured or partially captured authorizations to release unused funds. The gateway automatically calculates the reversible amount to prevent over-reversals.

Benefits

- Releases unused funds quickly
- Improves the customer experience
- Reduces disputes
- Helps meet card network compliance rules

Network Tokens for Card-on-File for Prosa

Products Included: Payments Processing

Region/Country: Mexico

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 226102

Mandate: Does not apply.

Description

This release will extend network token support for Card-on-File (COF) transactions by leveraging the existing merchant-initiated card-on-file (MITCOF) framework. Card-on-file transactions will be processed consistently for both PANs and network tokens and automatically populate the required network-specific token data when a network token is used.

Merchant Impact

Merchants using card-on-file transactions will be able to process network token credentials using the same MITCOF framework as PAN-based cards, without changing existing integration behavior. When network tokens are used, the required network token data will be automatically populated and sent as part of the authorization request. No merchant action will be required.

Benefits

- Enables full COF support for network tokens on Prosa.
- Ensures consistent MIT and COF processing regardless of credential type (PAN or network token).
- Improves authorization reliability for recurring and merchant-initiated transactions.
- Aligns Prosa processing with network token standards for Visa and Mastercard.

Recurring Billing Payment Date

Products Included: Recurring Billing

Region/Country: Global

Expected Release Date: RELEASE CANDIDATE | Q4 FY26

Internal Feature Number: 25444

Mandate: Does not apply

Description

This release will enable merchants to edit the payment date of a Recurring Billing subscription.

Merchant Impact

- Merchants can change the next billing date for an existing subscription with a status of Active, Delinquent, or Suspended by using the Edit Subscription page. This change updates the next billing date only and does not affect the subscription start date.
- When the billing date is changed, the next scheduled payment is automatically canceled and marked as canceled in the payment history. If the new billing date falls in the middle of a billing cycle, the next payment is prorated to charge only for the remaining days in that cycle. For example, if the original billing date is March 1 and the new billing date is the 15th, the next payment is prorated to cover April 1 through April 14.
- For installment subscriptions, the subscription end date is adjusted to keep the total number of payments the same and ensure the total charged amount does not increase or decrease. After the billing date is changed, merchants must send a new notification to the customer to inform them of the update.

Benefit

This update will provide the merchant's customers with more payment flexibility, preventing payment defaults.

Platform Upcoming Features

This section provides information about platform product enhancements and updates that are planned for future releases.

Branding AI Studio

Products Included: Branding AI Studio

Region/Country: All

Expected Release Date: RELEASE CANDIDATE | May 2026

Internal Feature Number: 28523

Mandate: Does not apply.

Description

The Branding AI Studio is a tool in the Business Center that enables Cybersource partners to customize the visual appearance of your partner portal. It enables you to upload a screenshot image of your business website, which it then analyzes and generates a portfolio theme. You can then review and edit the theme before saving it.

Benefit

Creating a branded portal aligns your merchant-facing experience with your brand.

It also enables you to:

- Create custom branding themes to meet your organizational needs.
- Obtain branded or co-branded URLs, custom branded login screens, and branded emails.
- Assign portfolio administrators who can manage your branding settings.
- Reduce the development costs of creating a custom website.

Merchant Impact

Merchants can access your customized portal using a branded URL.

Visa Dialect Font for Partner Branding Settings

Products Included: Branding settings in Branding AI Studio

Region/Country: Global

Expected Release Date: RELEASE CANDIDATE | June 2026

Internal Feature Number: PGMGMT-614

Mandate: Does not apply.

Description

The Visa Dialect font option is now available as a branding setting for all partners.

Merchant Impact

Partners can choose to apply the Visa Dialect font option in the Branding AI Studio settings. It does not affect partners who use customized branding settings.

Benefit

This new font option aligns partner portals with the Visa brand identity for Visa Acceptance Solutions partners who use the default branding settings.

Webhook Delivery Failure Notifications to Portfolio Contacts

Products Included: Webhooks

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | Q3 FY26

Internal Feature Number: 161438

Mandate: Does not apply

Description

Portfolio owners are subscribed to failure notification emails if one of their merchants has an inactive webhook URL. When Cybersource attempts to send a webhook notification to a merchant's inactive URL, an email is sent to the portfolio owner's email address. An email is sent when the webhook subscription's retry policy has reached its maximum number of retry attempts. The email address that Cybersource chooses to enroll in the email subscription is determined in this order of priority:

1. Business email address
2. Technical email address
3. Recovery email address

Merchant Impact

Merchants can expect to receive fewer emails regarding their webhook URL statuses.

Benefit

This update alerts portfolio owners and their support team when one of their merchant's webhook URLs cannot receive a webhook notification. Portfolio owners and their support team can monitor their merchants' webhook subscriptions from one email address.

Eight Digit BIN Support

Products Included: Transaction Management

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | July 2026

Internal Feature Number: 31631

Mandate: Does not apply

Description

This enhancement expands the Bank Identification Number (BIN) displayed on the Transaction Details page in Business Center from six digits to eight digits. Displaying the full eight-digit BIN provides more precise information about the issuing bank and card program. A new user permission controls access to this enhanced view. Users without this permission will continue to see the six-digit BIN.

Merchant Impact

Merchants can choose which users will be able to view the eight-digit BIN when they assign the new permission. This provides greater control over BIN visibility while enabling risk, operations, and support teams to access more detailed card-issuer information when needed. No changes are required for existing workflows, and transactions associated with six-digit BINs continue to display as they currently do.

Benefits

With this enhancement, merchants gain these benefits:

- Enhanced issuer and card program visibility: Displays the full eight-digit issuing BIN on the Transaction Details page, enabling more precise identification of issuing banks and card products than the legacy six-digit BIN.
- Improved reporting and analysis: Provides greater BIN-level granularity for transaction review, reconciliation, and trend analysis, supporting more accurate insights across card programs and issuers.
- Stronger fraud and risk management: Enables merchants to analyze and assess transactions using more specific BIN data, helping refine risk reviews and reduce ambiguity when multiple products share the same six-digit prefix.
- Operational efficiency for support and investigations: Helps customer support and operations teams more quickly identify the exact card program involved in a transaction when researching declines, disputes, or inquiries.
- Alignment with industry standards: Supports the industry-wide migration to eight-digit issuing BINs, ensuring that merchants see complete BIN information for newly issued cards.

New Report Metadata

Products Included: Reports

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 121008

Mandate: Does not apply

Description

Report metadata will be available when you access reports through the reporting API. This metadata includes key details such as file size and record count, enabling the viewer to understand the expected volume of a report before downloading it. The metadata is available in these locations:

- Response headers when reports are downloaded using `/reporting/v3/report-downloads`
- Response body when report details are retrieved using `/reporting/v3/reports`

Merchant Impact

By viewing report size and record count in advance, you can make informed decisions about when and how to retrieve reports. This enables you to proactively adjust processing settings such as timeouts, memory allocation, or batching logic before starting a download, reducing the risk of failed or inefficient report processing.

Benefits

This enhancement will provide the following benefits:

- Improved reliability: Reduces failed downloads and timeouts caused by unexpectedly large reports.
- Greater processing efficiency: Optimizes report handling without trial-and-error retries.
- Better integration control: Helps you plan resource usage and batching strategies in advance.
- Reduced operational overhead: Eliminates the need to download or parse report files just to determine their size or record volume.

New Incident Detail Report

Products Included: Reports

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | May 2026

Internal Feature Number: 223732

Mandate: Does not apply

Description

The new Incident Detail report provides a single, consolidated view of transaction activity related to a specific processing incident. This report brings together standardized transaction data that otherwise must be collected manually from multiple sources. The Incident Detail report is a one-time, incident-specific report available through Business Center or the Reporting API (definitionName:IncidentDetailClass).

Merchant Impact

After a processing incident, merchants can enjoy these advantages:

- Quick identification of affected transactions, such as potential duplicate payments or transactions that did not settle as expected.
- Less time and effort spent gathering, reconciling, and validating transaction data.
- A consistent, incident-focused view of transaction activity without manual data compilation.

Benefits

This enhancement provides these benefits:

- **Faster incident investigation:** All relevant transaction details in a single report.
- **Simplified reconciliation:** Less manual effort validating transaction outcomes.
- **Improved visibility:** Clearer insight into affected activity, including cross-border transactions.
- **Flexible access:** The report runs directly in the Business Center or through the reporting API.

New Cross-Border Report

Products Included: Reports

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | May 2026

Internal Feature Number: 224831

Mandate: Does not apply

Description

A new Cross-Border Transactions report provides a single, consolidated view of all cross-border transactions. This report highlights key transaction details specifically for cross-border payments, helping track, review, and reconcile international transactions.

The report is available through Business Center or the reporting API (definitionName: CrossBorderDetailClass).

Merchant Impact

The new report focuses entirely on cross-border activity which eliminates the need to filter or combine data from multiple reports. This report simplifies day-to-day reconciliation and makes it easier to investigate international transactions.

Benefits

The Cross-Border Report provides:

- Faster reconciliation: Quickly review cross-border transactions in one report without manual data filtering.
- Improved visibility: Gain a clearer, more consistent view of international payment activity.
- Operational efficiency: Save time spent compiling data from multiple sources.
- Flexible access: Use the report directly in the Business Center or integrate it through the reporting API.

OAuth 2.0 New Setup Methods

Products Included: OAuth 2.0

Country/Region: Global

Expected Release Date: June 2026

Description

Cybersource offers OAuth 2.0 to organizations who are contracted as an acquirer, merchant, or technology partner. OAuth 2.0 is a token-based method for securely exchanging information between your organization and another in order to act on behalf of the organization, access their data, or consent to other organizations accessing your systems.

Acquirer Impact

Acquirers can set up OAuth 2.0 in order to access merchant data from merchants in their portfolio.

Merchant Impact

Merchants can set up OAuth 2.0 in their payment systems for one of these purposes:

- Enable technology partners to act on-behalf of the merchant in order to process payments or other API related tasks.
- Enable their managing acquirer to access merchant data.

Technology Partner Impact

Technology partners can add OAuth 2.0 into their integration solution. This enables merchants to register and allow the solution to act on their behalf.

Benefit

Allowing all three organization types the ability to set up OAuth 2.0 through Cybersource enables all organizations to self-set up without relying on outside parties to enable OAuth 2.0. Previously, Cybersource offered OAuth 2.0 only to technology partners.

REST Client SDK Update for Node, PHP, Python, and Ruby

Products Included: REST Client SDK

Region/Country: All

Expected Release Date: | June 2026

Internal Feature Number: 193763

Mandate: Does not apply.

Description

The REST Client SDK will support the new JSON Web Token (JWT) message construction and Message-Level Encryption (MLE) enablement requirements for these programming languages:

- Node
- PHP
- Python
- Ruby

Warning:

To avoid potential transaction failures, portfolio owners must enable this updated version of MLE for their merchants by **September 2026**.

Benefit

The REST Client SDK provides merchants with an alternative method to integrating to Cybersource REST APIs. This method enables merchants to send and receive REST API messages using REST Client SDK instead of creating a custom set up.

The updated SDK also keeps merchants in compliance with the new JWT-based message construction and updated MLE requirements.

Merchant Impact

Merchants already using the REST Client SDK should update to the newest SDK version to remain in compliance.

Warning: You risk transaction failures if you do not update your system to support the new JSON Web Token (JWT) message construction and Message-Level Encryption (MLE) enablement requirements.

Risk Management Upcoming Features

This section provides information about risk management product enhancements and updates that are planned for future releases.

New Declined Payment Status to Be Added to Fraud Management Essentials

Products Included: Fraud Management Essentials

Region/Country: Global

Expected Release Date: RELEASE CANDIDATE | June 2026

Internal Feature Number: 17231

Mandate: Does not apply

Description

For all transactions that are screened by Fraud Management Essentials (FME), a new *declined* status will be generated for any transaction that invokes a decline or error response from the card issuer. These transactions are not currently included in FME. This status will be final and will not be subsequently editable. The introduction of this new status will allow:

- Issuer-declined transactions to appear in FME Order Search query results and Order Details.
- Issuer-declined transactions to be subject to marking tool functionality.
- Issuer-declined transactions to be included in total transaction volume across relevant FME reports and reporting capabilities.

Merchant Impact

By identifying issuer declines and errors, merchants will be able to track issuer decline rates and detect changes that can adversely impact their payments.

Restrict List Sharing Control in Decision Manager

Products Included: Decision Manager

Region/Country: Global

Expected Release Date: RELEASE CANDIDATE | June 2026

Internal Feature Number: 188520

Mandate: Does not apply

Description

Restrict List Sharing is a new optional privacy control for organizations using Decision Manager Hierarchy (DMH). Currently, all positive, negative, and review lists within a DMH family are automatically shared across member organizations. With this enhancement, each organization chooses whether to share its lists or keep them private, supporting regional privacy requirements such as those in Europe while maintaining the benefits of DMH. This feature is in final testing.

Merchant Impact

This optional feature enables DMH merchants to choose with whom they share their lists. They may choose to keep it private or to share it with their parent organization (merchant organization or portfolio organization).

Benefit

Organizations gain control over list sharing to meet privacy requirements while maintaining the collaborative fraud prevention benefits of Decision Manager Hierarchy.

New Declined Status for Decision Manager

Products Included: Decision Manager

Region/Country: Global

Expected Release Date: RELEASE CANDIDATE | June 2026

Internal Feature Number: 17233

Mandate: Does not apply

Description

A new *declined* status will be available in Decision Manager. This status applies to all transactions in which any service running between pre-authorization and post-authorization results in a decline or error, including authorization declines. This status is final and cannot be subsequently updated.

Key features of the *declined* status:

- **Case search visibility**: Transactions with the new *declined* status appear in case search query results.
- **Marking tool functionality**: These transactions are subject to the marking tool functionality.
- **Report inclusion**: The status is counted toward the total number of transactions in reports and included in applicable reports.

Merchant Impact

Transactions with the new *declined* status:

- Appear in case search query results
- Appear in Similar Search search results with *declined* status
- Are eligible for marking tool functionality
- Are counted toward total transaction volume in reporting
- Are included in all relevant reports

Benefit

- **Improved Visibility**: Previously, transactions affected by declines such as authorization declines were not visible in case search, although they could be viewed in Transaction Details as billable transactions without risk-related data (for example, score, info codes). This provides more transparency around Decision Manager's processing of these transactions.
- **Enhanced Marking Ability**: With the new status, merchants can mark these types of transactions as suspect.
- **Better Fraud Detection**: An unusually high number of declined transactions is more noticeable, enabling quicker investigation and resolution.

Improve Decision Manager Accuracy through Standard API Fields

Products Included: Decision Manager

Region/Country: Global

Expected Release Date: RELEASE CANDIDATE | June 2026

Internal Feature Number: 32281

Mandate: Does not apply

Description

This feature extends the Decision Manager (DM) API to support more standard request fields, reducing the reliance on custom fields. The new fields are available across Decision Manager capabilities, including custom rules, velocity, lists, case management, and reporting.

Merchant Impact

The new standard API fields are optional. If a merchant chooses to use the new fields, they can send some or all data in these new fields by updating their integration accordingly.

If a merchant migrates from using a merchant-defined data (MDD) field to a new API field, they should update any associated rules, velocities, cases, lists, or reports to help ensure their fraud strategy continues to operate as intended.

Existing MDD fields continue to be supported. This enhancement is fully backward compatible and requires no mandatory changes. Merchants may continue using their current integration.

Benefits

This enhancement improves fraud detection accuracy by standardizing data inputs. It also enhances model scoring accuracy by enabling these fields to be consumed by the risk model.

3-D Secure Data-Only for TSYS Acquiring Solutions

Products Included: Payment Processing

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Numbers: 161346 & 28040

Mandate: Does not apply

Description

The 3-D Secure Data-Only transactions for TSYS Acquiring Solutions feature enables the submission of 3-D Secure authentication data for informational and risk assessment purposes without triggering an authentication challenge. This capability is delivered with a feature toggle that is disabled by default.

Merchant Impact

There is no immediate impact on merchants, as the feature is released with the feature toggle turned off. Merchants will be notified before the feature is activated. No action is required at this time.

Benefit

- Enables submission of 3-D Secure data for risk scoring and downstream analysis
- Supports alignment with TSYS Acquiring Solutions processing capabilities
- Provides flexibility to enable 3-D Secure Data-Only processing when appropriate

Visa Protect Risk Insights (VPRI)

Products Included: Visa Protect Risk Insights

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | September 2026

Internal Feature Number: 32281

Mandate: Does not apply

Description

Visa Protect Risk Insights (VPRI) is an API-only solution that delivers a transaction risk score and actionable insights. Built on Visa's global data and AI, VPRI provides enhanced visibility into customer behavior and transaction risk, enabling clients to strengthen and enrich their existing fraud management solutions and AI models rather than replace them. VPRI is a network-agnostic, AI-powered risk solution that applies across industries and use cases beyond payments.

Client Impact

Clients integrate VPRI as an additional layer of visibility within existing fraud management systems or AI models, enriching risk evaluation without disruption.

Benefits

VPRI provides these benefits:

- Brings Visa's global visibility into each transaction, enabling more confident decisions.
- Adds depth to existing fraud management systems and AI models, improving accuracy of decisions.
- Increases approval of legitimate transactions, capturing revenue that would otherwise be lost.

Technical Partner Upcoming Features

This section provides information about technical partner product enhancements and updates that are planned for future releases.

Adobe Commerce REST API Integration: Response MLE

Products Included: Adobe Commerce REST API integration

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 181565

Mandate: Does not apply

Description

Our platform already supports MLE for incoming transaction requests from ISV integrations. This new capability will extend that same protection to *incoming transaction responses*, providing merchants with end-to-end encryption across the full transaction flow.

The solution uses strong industry-standard encryption protocols to provide a high level of protection for sensitive payment data as it moves between our platform and merchant environments.

- RSA-OAEP-256 for secure key exchange
- AES-GCM 256-bit for payload encryption

With this enhancement, merchants securely receive and decrypt transaction responses using their own Response MLE certificate in their back-office systems. This update helps ensure that transaction data stays private, protected, and unchanged from the moment it is sent to the moment it is received.

Merchant Impact

To use this feature, merchants must complete these prerequisites:

- Install the latest version of the ISV integration that supports Response MLE.
- Upload their REST API Response MLE certificate in the back office.
- Configure their system to decrypt and display the encrypted transaction response data.

Merchants can continue using their current REST key and shared secret and adopt MLE later when ready.

Benefits

With this enhancement, merchants gain these benefits:

- A secure place in the back office to store their Response MLE certificate.
- Automatic encryption of all response messages using the merchant's public key.
- The ability to decrypt transaction details using their private key.
- Full compatibility with existing MLE request-side encryption.
- Support for industry-standard JOSE JWE/JWS structures.
- Stronger security that prevents unauthorized access, interception, or alteration of transaction details.
- Compliance readiness that meets Visa's upcoming 2026 encryption mandate for ISV-integrated merchants.
- Accurate and trusted data that ensures that the response information displayed in back-office systems or to customers is authentic and verified.
- Future proofing so that early adopters avoid the rush and potential disruption when the requirement becomes mandatory.

This enhancement gives merchants a stronger, future-ready security foundation and ensures that they are fully aligned with Visa's 2026 requirements while maintaining a smooth, trusted payment experience for their customers.

Commercetools: Response MLE

Products Included: Commercetools

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 181580

Mandate: Does not apply

Description

Our platform already supports MLE for incoming transaction requests from ISV integrations. This new capability extends that same protection to *incoming transaction responses*, providing merchants with end-to-end encryption across the full transaction flow.

The solution uses strong industry-standard encryption protocols to provide a high level of protection for sensitive payment data as it moves between our platform and merchant environments.

- RSA-OAEP-256 for secure key exchange
- AES-GCM 256-bit for payload encryption

With this enhancement, merchants will securely receive and decrypt transaction responses using their own Response MLE certificate in their back-office systems. This update helps ensure transaction data stays private, protected, and unchanged from the moment it is sent to the moment it is received.

Merchant Impact

To use this feature, merchants must complete these prerequisites:

- Install the latest version of the ISV integration that supports Response MLE.
- Upload their REST API Response MLE certificate in the back office.
- Configure their system to decrypt and display the encrypted transaction response data.

Merchants can continue using their current REST key and shared secret and adopt MLE later when ready.

Benefits

With this enhancement, merchants gain these benefits:

- A secure place in the back office to store their Response MLE certificate.
- Automatic encryption of all response messages using the merchant public key.
- The ability to decrypt transaction details using their private key.
- Full compatibility with existing MLE request-side encryption.
- Support for industry-standard JOSE JWE/JWS structures.
- Stronger security that prevents unauthorized access, interception, or alteration of transaction details.
- Compliance readiness that meets Visa's upcoming 2026 encryption mandate for ISV-integrated merchants.
- Accurate and trusted data that ensures that the response information displayed in back-office systems or to customers is authentic and verified.
- Future proofing so that early adopters avoid the rush and potential disruption when the requirement becomes mandatory.

This enhancement gives merchants a stronger, future-ready security foundation and ensures that they are fully aligned with Visa's 2026 requirements while maintaining a smooth, trusted payment experience for their customers.

OpenCart: Response MLE

Products Included: OpenCart

Region/Country: AP, CEMEA, EU, LAC, NA

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 214199

Mandate: Does not apply

Description

Our platform already supports MLE for incoming transaction requests from ISV integrations. This new capability will extend that same protection to *incoming transaction responses*, providing merchants with end-to-end encryption across the full transaction flow.

The solution uses strong industry-standard encryption protocols to provide a high level of protection for sensitive payment data as it moves between our platform and merchant environments.

- RSA-OAEP-256 for secure key exchange
- AES-GCM 256-bit for payload encryption

With this enhancement, merchants will securely receive and decrypt transaction responses using their own Response MLE certificate in their back-office systems. This update helps ensure transaction data stays private, protected, and unchanged from the moment it is sent to the moment it is received.

Merchant Impact

To use this feature, merchants will need to complete these prerequisites:

- Install the latest version of the ISV integration that supports Response MLE.
- Upload their REST API Response MLE certificate in the back office.
- Configure their system to decrypt and display the encrypted transaction response data.

Merchants can continue using their current REST key and shared secret and adopt MLE later when ready.

Benefits

With this enhancement, merchants gain these benefits:

- A secure place in the back office to store their Response MLE certificate.
- Automatic encryption of all response messages using the merchant public key.
- The ability to decrypt transaction details using their private key.
- Full compatibility with existing MLE request-side encryption.
- Support for industry-standard JOSE JWE/JWS structures.
- Stronger security that prevents unauthorized access, interception, or alteration of transaction details.
- Compliance readiness that meets Visa's upcoming 2026 encryption mandate for ISV-integrated merchants.
- Accurate and trusted data that ensures that the response information displayed in back-office systems or to customers is authentic and verified.
- Future proofing so that early adopters avoid the rush and potential disruption when the requirement becomes mandatory.

This enhancement gives merchants a stronger, future-ready security foundation and ensures that they are fully aligned with Visa's 2026 requirements while maintaining a smooth, trusted payment experience for their customers.

Oracle NetSuite: PayPal v2 and Venmo

Products Included: Oracle NetSuite

Region/Country: AP, CEMEA, EU, LAC, NA

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 209483

Mandate: Does not apply

Description

Merchants using PayPal v2 or Venmo will be able to manage the full payment cycle directly through the SuiteApp, while merchants currently using PayPal v1 will continue to operate without disruption. These payment types include capture, refund, and reversal.

Merchant Impact

Merchants will expand payment choice while maintaining a smooth and reliable operational experience.

- Existing PayPal v1 processing will remain unchanged.
- Merchants who adopt PayPal v2 or Venmo will have full-payment lifecycle support.

Benefit

This update will provide these benefits:

- Access to More Payment Options: In addition to existing PayPal v1 setups, merchants will be able support PayPal v2 and Venmo.
- No Disruption for Existing Merchants: Merchants currently using PayPal v1 will be able to continue operating as they do, with no impact to their existing integration.
- Reliable Payment Operations: Capture, refund, and authorization reversal actions will be handled consistently across supported PayPal and Venmo payment types.
- Reduced Support Issues: Explicit routing will reduce the risk of requests being misdirected, helping to avoid unnecessary payment errors and support escalations.

PrestaShop: Response MLE

Products Included: PrestaShop

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 181567

Mandate: Does not apply

Description

Our platform already supports MLE for incoming transaction requests from ISV integrations. This new capability will extend that same protection to *incoming transaction responses*, providing merchants with end-to-end encryption across the full transaction flow.

The solution uses strong industry-standard encryption protocols to provide a high level of protection for sensitive payment data as it moves between our platform and merchant environments.

- RSA-OAEP-256 for secure key exchange
- AES-GCM 256-bit for payload encryption

With this enhancement, merchants will securely receive and decrypt transaction responses using their own Response MLE certificate in their back-office systems. This update helps ensure transaction data stays private, protected, and unchanged from the moment it is sent to the moment it is received.

Merchant Impact

To use this feature, merchants must complete these prerequisites:

- Install the latest version of the ISV integration that supports Response MLE.
- Upload their REST API Response MLE certificate in the back office.
- Configure their system to decrypt and display the encrypted transaction response data.

Merchants can continue using their current REST key and shared secret and adopt MLE later.

Benefits

With this enhancement, merchants gain these benefits:

- A secure place in the back office to store their Response MLE certificate.
- Automatic encryption of all response messages using the merchant public key.
- The ability to decrypt transaction details using their private key.
- Full compatibility with existing MLE request-side encryption.
- Support for industry-standard JOSE JWE/JWS structures.
- Stronger security that prevents unauthorized access, interception, or alteration of transaction details.
- Compliance readiness that meets Visa's upcoming 2026 encryption mandate for ISV-integrated merchants.
- Accurate and trusted data that ensures that the response information displayed in back-office systems or to customers is authentic and verified.
- Future proofing so that early adopters avoid the rush and potential disruption when the requirement becomes mandatory.

This enhancement provides merchants with a stronger, future-ready security foundation and ensures that they are fully aligned with Visa's 2026 requirements while maintaining a smooth, trusted payment experience for their customers.

Salesforce B2B/D2C: Response MLE

Products Included: Salesforce B2B/D2C

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 181568

Mandate: Does not apply

Description

Our platform already supports MLE for incoming transaction requests from ISV integrations. This new capability will extend that same protection to *incoming transaction responses*, providing merchants with end-to-end encryption across the full transaction flow.

The solution uses strong industry-standard encryption protocols to provide a high level of protection for sensitive payment data as it moves between our platform and merchant environments.

- RSA-OAEP-256 for secure key exchange
- AES-GCM 256-bit for payload encryption

With this enhancement, merchants will securely receive and decrypt transaction responses using their own Response MLE certificate in their back-office systems. This update helps ensure transaction data stays private, protected, and unchanged from the moment it is sent to the moment it is received.

Merchant Impact

To use this feature, merchants will need to complete these prerequisites:

- Install the latest version of the ISV integration that supports Response MLE.
- Upload their REST API Response MLE certificate in the back office.
- Configure their system to decrypt and display the encrypted transaction response data.

Merchants can continue using their current REST key and shared secret and adopt MLE later when ready.

Benefits

With this enhancement, merchants will gain these benefits:

- A secure place in the back office to store their Response MLE certificate.
- Automatic encryption of all response messages using the merchant public key.
- The ability to decrypt transaction details using their private key.
- Full compatibility with existing MLE request-side encryption.
- Support for industry-standard JOSE JWE/JWS structures.
- Stronger security that prevents unauthorized access, interception, or alteration of transaction details.
- Compliance readiness that meets Visa's upcoming 2026 encryption mandate for ISV-integrated merchants.
- Accurate and trusted data that ensures that the response information displayed in back-office systems or to customers is authentic and verified.
- Future proofing so that early adopters avoid the rush and potential disruption when the requirement becomes mandatory.

This enhancement gives merchants a stronger, future-ready security foundation and ensures that they are fully aligned with Visa's 2026 requirements while maintaining a smooth, trusted payment experience for their customers.

Salesforce B2C Commerce REST API Integration: Meta-Key Support

Products Included: Salesforce B2C Commerce REST API Integration

Region/Country: AP, CEMEA, EU, LAC, NA

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 214710

Mandate: Does not apply

Description

The Salesforce B2C Commerce REST API integration will be enhanced to support Meta-Key authentication for merchants using either:

- REST shared secret
- Certificate-based key

Some merchants manage complex account structures, such as a top-level merchant account with multiple sub-accounts. In these cases, Meta-Key authentication will need to be enabled only at the top-level account.

Adding Meta-Key support directly into the REST API integration, will make managing authentication easier for larger merchants, and it will reduce the need for custom setup or manual workarounds.

Merchants will be able to turn Meta-Key on or off through a new setting in Salesforce Business Manager which is located in **Merchant Tools > Site Preferences > Custom Preferences > Cybersource Core**

This setting will enable the integration to correctly identify and use the authentication method configured for these services.

Merchant Impact

The default setting will remain **Meta-Key disabled**, so current configurations can continue to work as they do unless a merchant enables the feature.

- A new Meta-Key setting will be added in Cybersource Core
- If both authentication models are supported in the final design, merchants will see a key type selection.
- If Meta-Key is not enabled, no change to existing behavior will occur.

Benefits

This update has these benefits:

- **Simpler Enterprise Authentication**: Merchants will use Meta-Key authentication without requiring custom development or making special changes to the cartridge.
- **Clearer Setup Experience**: A dedicated setting in the Cybersource Core will make it easier to understand how authentication is configured and what type of key material is used.
- **Better Support for Complex Account Structures**: Merchants with parent and child account models will be able to manage Meta-Key usage more effectively, especially where authentication is controlled at the top account level.

Salesforce B2C REST API Integration: Response MLE

Products Included: Salesforce B2C REST API integration

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 181557

Mandate: Does not apply

Description

Our platform already supports MLE for incoming transaction requests from ISV integrations. This new capability will extend that same protection to *incoming transaction responses*, providing merchants with end-to-end encryption across the full transaction flow.

The solution uses strong industry-standard encryption protocols to provide a high level of protection for sensitive payment data as it moves between our platform and merchant environments.

- RSA-OAEP-256 for secure key exchange
- AES-GCM 256-bit for payload encryption

With this enhancement, merchants will securely receive and decrypt transaction responses using their own Response MLE certificate in their back-office systems. This update helps ensure transaction data stays private, protected, and unchanged from the moment it is sent to the moment it is received.

Merchant Impact

To use this feature, merchants will need to complete these prerequisites:

- Install the latest version of the ISV integration that supports Response MLE.
- Upload their REST API Response MLE certificate in the back office.
- Configure their system to decrypt and display the encrypted transaction response data.

Merchants can continue using their current REST key and shared secret and adopt MLE later when ready.

Benefits

With this enhancement, merchants gain these benefits:

- A secure place in the back office to store their Response MLE certificate.
- Automatic encryption of all response messages using the merchant public key.
- The ability to decrypt transaction details using their private key.
- Full compatibility with existing MLE request-side encryption.
- Support for industry-standard JOSE JWE/JWS structures.
- Stronger security that prevents unauthorized access, interception, or alteration of transaction details.
- Compliance readiness that meets Visa's upcoming 2026 encryption mandate for ISV-integrated merchants.
- Accurate and trusted data that ensures that the response information displayed in back-office systems or to customers is authentic and verified.
- Future proofing so that early adopters avoid the rush and potential disruption when the requirement becomes mandatory.

This enhancement gives merchants a stronger, future-ready security foundation and ensures that they are fully aligned with Visa's 2026 requirements while maintaining a smooth, trusted payment experience for their customers.

Salesforce B2C Simple Order API Integration: Venmo

Products Included: Salesforce B2C Simple Order API integration

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 22526

Mandate: Does not apply

Description

Upcoming enhancements to the Salesforce B2C Commerce integration add Venmo as a payment option, using the Simple Order API to work seamlessly with existing setups.

Merchant Impact

These updates deliver a simpler, more up-to-date checkout experience in Salesforce B2C Commerce, helping merchants increase payment choice while keeping setup and ongoing management easy.

Benefit

This enhancement will provide these benefits:

- Venmo checkout support (US only): Offer customers the option to pay with Venmo for a faster, familiar checkout experience.
- Easy configuration: Enable Venmo directly in Salesforce Business Manager. No custom development will be required.
- No credential management: Visa handles onboarding and credentials, reducing setup effort and improving security.
- Full transaction support: Venmo transactions support order creation, authorization, capture, sale, reversals, status checks, and refunds.
- Smooth checkout experience: Venmo buttons appear automatically when enabled, with support for redirects and line-item details.

Salesforce Order Management: Response MLE

Products Included: Salesforce Order Management

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 181578

Mandate: Does not apply

Description

Our platform already supports MLE for incoming transaction requests from ISV integrations. This new capability will extend that same protection to *incoming transaction responses*, providing merchants with end-to-end encryption across the full transaction flow.

The solution uses strong industry-standard encryption protocols to provide a high level of protection for sensitive payment data as it moves between our platform and merchant environments.

- RSA-OAEP-256 for secure key exchange
- AES-GCM 256-bit for payload encryption

With this enhancement, merchants will securely receive and decrypt transaction responses using their own Response MLE certificate in their back-office systems. This update helps ensure transaction data stays private, protected, and unchanged from the moment it is sent to the moment it is received.

Merchant Impact

To use this feature, merchants must complete these prerequisites:

- Install the latest version of the ISV integration that supports Response MLE.
- Upload their REST API Response MLE certificate in the back office.
- Configure their system to decrypt and display the encrypted transaction response data.

Merchants can continue using their current REST key and shared secret and adopt MLE later when ready.

Benefits

With this enhancement, merchants gain these benefits:

- A secure place in the back office to store their Response MLE certificate.
- Automatic encryption of all response messages using the merchant public key.
- The ability to decrypt transaction details using their private key.
- Full compatibility with existing MLE request-side encryption.
- Support for industry-standard JOSE JWE/JWS structures.
- Stronger security that prevents unauthorized access, interception, or alteration of transaction details.
- Compliance readiness that meets Visa's upcoming 2026 encryption mandate for ISV-integrated merchants.
- Accurate and trusted data that ensures that the response information displayed in back-office systems or to customers is authentic and verified.
- Future proofing so that early adopters avoid the rush and potential disruption when the requirement becomes mandatory.

This enhancement gives merchants a stronger, future-ready security foundation and ensures that they are fully aligned with Visa's 2026 requirements while maintaining a smooth, trusted payment experience for their customers.

SAP DPA: Apple Pay and Google Pay Update

Products Included: SAP DPA

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 28406

Mandate: Does not apply

Description

The SAP DPA integration will be updated to support the correct recognition of Apple Pay and Google Pay transactions and ensure that they are processed according to SAP's API standards.

Merchant Impact

When enabled, the system will fully support Apple Pay and Google Pay transactions that are sent by SAP as external payments, including:

- Capturing funds
- Processing refunds
- Voiding transactions, where relevant

Benefits

The SAP DPA integration update will ensure that Apple Pay and Google Pay transactions are identified properly and processed correctly, providing smoother payment handling and compatibility with SAP APIs.

WooCommerce: Response MLE

Products Included: WooCommerce

Region/Country: Global

Expected Release Date: IN DEVELOPMENT | June 2026

Internal Feature Number: 181581

Mandate: Does not apply

Description

Our platform already supports MLE for incoming transaction requests from ISV integrations. This new capability will extend that same protection to *incoming transaction responses*, providing merchants with end-to-end encryption across the full transaction flow.

The solution uses strong industry-standard encryption protocols to provide a high level of protection for sensitive payment data as it moves between our platform and merchant environments.

- RSA-OAEP-256 for secure key exchange
- AES-GCM 256-bit for payload encryption

With this enhancement, merchants will securely receive and decrypt transaction responses using their own Response MLE certificate in their back-office systems. This update helps ensure transaction data stays private, protected, and unchanged from the moment it is sent to the moment it is received.

Merchant Impact

To use this feature, merchants must complete these prerequisites:

- Install the latest version of the ISV integration that supports Response MLE.
- Upload their REST API Response MLE certificate in the back office.
- Configure their system to decrypt and display the encrypted transaction response data.

Merchants can continue using their current REST key and shared secret and adopt MLE later when ready.

Benefits

With this enhancement, merchants will gain these benefits:

- A secure place in the back office to store their Response MLE certificate.
- Automatic encryption of all response messages using the merchant public key.
- The ability to decrypt transaction details using their private key.
- Full compatibility with existing MLE request-side encryption.
- Support for industry-standard JOSE JWE/JWS structures.
- Stronger security that prevents unauthorized access, interception, or alteration of transaction details.
- Compliance readiness that meets Visa's upcoming 2026 encryption mandate for ISV-integrated merchants.
- Accurate and trusted data that ensures that the response information displayed in back-office systems or to customers is authentic and verified.
- Future proofing so that early adopters avoid the rush and potential disruption when the requirement becomes mandatory.

This enhancement gives merchants a stronger, future-ready security foundation and ensures that they are fully aligned with Visa's 2026 requirements while maintaining a smooth, trusted payment experience for their customers.

Features Released in April 2026

This section lists the features that were released in the previous month.

Table 2. Features Released in April 2026

Product(s)	Feature	Internal Feature Number
Batch Upload	New missing responses report	189385
Batch Upload	Enhanced batch processing completion email	--
Card-on-File and Recurring Transactions	Support for stored credentials transactions for Prosa	169302
Decision Manager	New reloadable/non-reloadable indicator field	107163
Installments	Support for meses sin intereses (months without interest) for Prosa	20448
Invoicing	Specific email address for merchant payment notifications	180830
Invoicing and Pay by Link	Custom transaction reference number	202000
OpenCart	Enhancements for the checkout experience	186517
Pay by Link	Custom data collection fields	107887
Pay by Link	Custom default settings	107888
Pay by Link	Support for tax and discount fixed-price payment links	158827
Payments Processing	3-D Secure Data-Only transactions for Rede	31967
Payments Processing	Automatic authorization reversal for Cielo	28055
Payments Processing	Staged digital wallets for Rede	25490
Payments Processing	Support for Mastercard Data Integrity Mandate AN6022 and AN4022 for Prosa	185839
PrestaShop	Support for Unified Checkout	195834
Salesforce B2C Simple Order API	Support for PayPal Version 2	188508
Shopify	Support for China UnionPay	158066
Token Management Service	Digital commerce authentication	32294

Table 2. Features Released in April 2026 (continued)

Product(s)	Feature	Internal Feature Number
Unified Checkout	Support for PayPal and Venmo	18067
Unified Checkout	New pass-through fields	31532
Unified Checkout	Regional wallet support	25525
Unified Checkout	Support for Apple Pay in India	27875

See the April 2026 Product Note for details about these features.