Kount Application

Platforms: Legacy eCommerce, KCCP eCommerce and eCommerce+OMS

Kount provides online services to determine the legitimacy and potential risk of orders submitted through your Kibo site(s). Kount reviews every order for suspicious or inconsistent data related to the customer's identity, credit card information, IP address and origin location, and the device and browser used. Kount uses the results of this analysis to calculate a fraud score. The service then assesses the risk of the order’s data and fraud score using rules you configure in Kount to identify potentially fraudulent orders.

The Kount application facilitates the transfer of order data between Kibo and Kount. After an order is reviewed in Kount, the app imports the fraud decision information back into Kibo eCommerce, updates the status of the order to Accepted or Rejected, and displays the Kount Fraud Detection Results in the Order Details in Admin. Throughout the fraud detection process, Kibo encrypts all sensitive customer data to ensure PCI compliance.

Application Features

- Automatically sends information about submitted orders to Kount, including the shopper's browser type, IP address, device type, billing information, etc.
- Validates shopper purchases against your Kount rules to determine fraud scores and legitimacy of the purchaser.
- Updates order status and details in eCommerce based on Kount fraud detection results.
- Avoids excessive overhead for low-value orders by allowing you to set a monetary threshold below which orders are NOT screened for fraud.

Install the App

For assistance installing the application, please reach out to your SI partner or Kibo's professional services and enablement team.

Configure the App

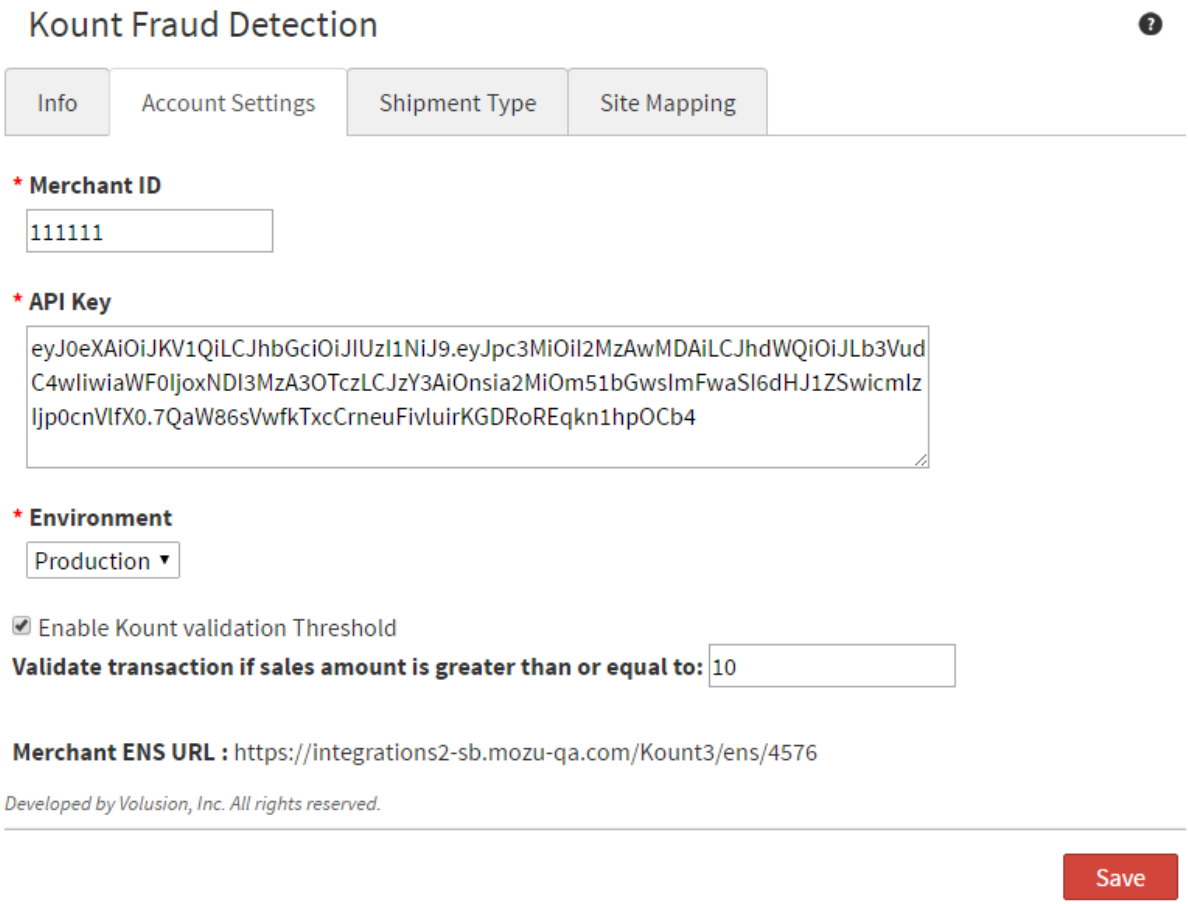
Review the configuration requirements to ensure you have everything you need to successfully configure the app.

Configuration Requirements

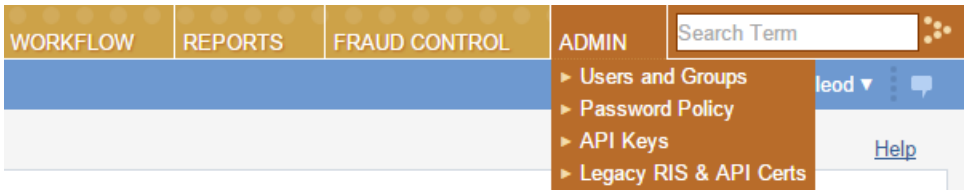
- An active Kount account.
- Your Kount **Merchant ID**. Kount provides this ID when you set up your Kount account.
- Your Kount **API Key**. If you don't have an API Key, the next section walks you through creating one in Kount.
- You must have access to modify and update your Kibo theme.
- The Kount application must be installed on your tenant.

Configure Kount Account Settings

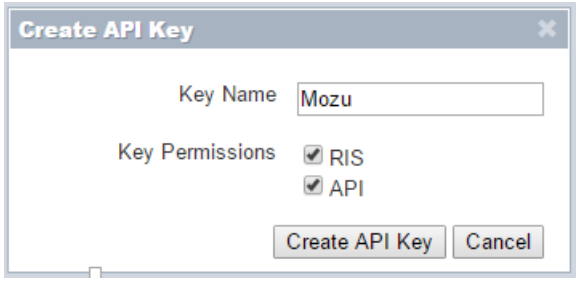
1. In Admin, go to **System** > **Customization** > **Applications**.
2. Click **Kount**.
3. Click the **Configuration** link to open configuration settings.
4. Go to the **Account Settings** tab:



5. Enter your Kount **Merchant ID**. Kount provides this ID when you set up your Kount account.
6. Enter your Kount **API Key**. To find or generate this key in Kount, navigate to **Admin** > **API Keys**:



The key you use must have both **RIS** and **API** permissions. You can configure key permissions when you create the key:

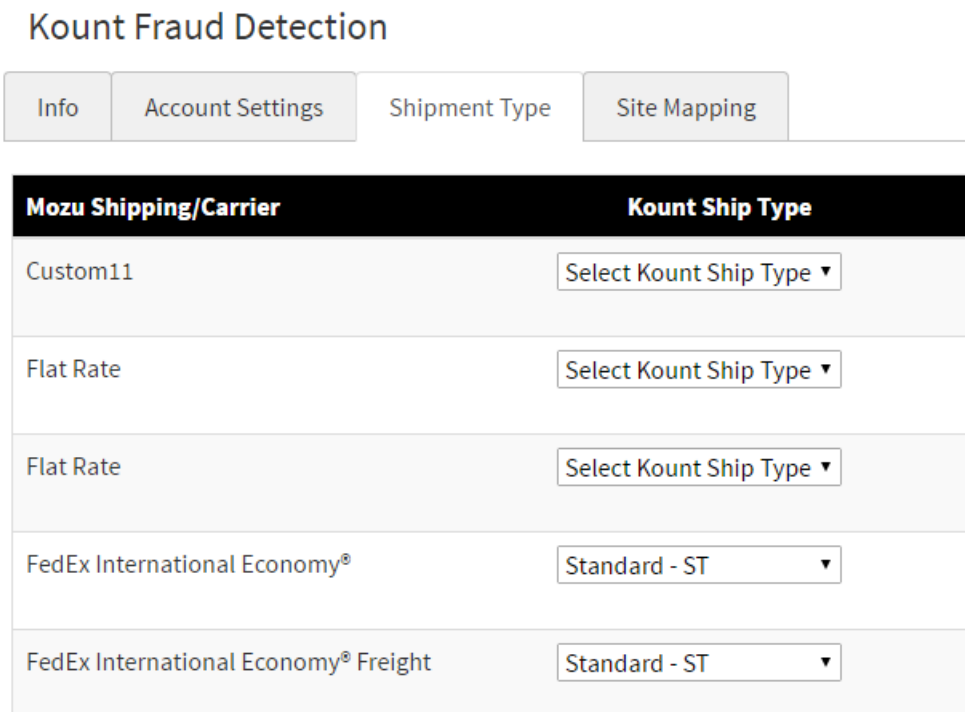


7. Select the Kount **Environment** you want to work in.
8. (Optional) Select **Enable Kount validation Threshold** to set a price threshold below which orders are not screened by Kount. For example, you may want Kount to only screen orders over $10 for fraud.
9. Click **Save**. This step connects eCommerce to your Kount account.

Configure Shipment Types

In this step of the configuration, you establish the mapping between shipment types in Kibo and those in Kount. You can then use this mapping within Kount to prioritize fraud screening based on an order's shipment type, so, for example, you may screen expedited shipment orders before orders with standard shipping.

1. Go to the **Shipment Types** tab:



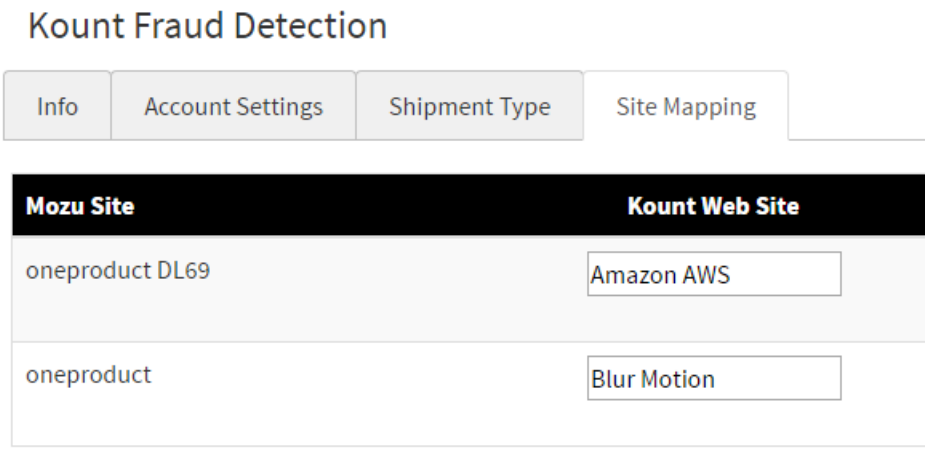
2. For each shipment type, select a corresponding shipment type in Kount from the dropdown menu.
3. Click **Save**.

After you complete this configuration, you can view the shipment type for incoming orders in Kount and prioritize them as you see fit. You can also configure your Kount rules to handle orders differently based on shipment type.

Configure Site Mappings

In this step of the configuration, you establish the mapping between sites in Kibo and those in Kount. You can then use this mapping within Kount to prioritize fraud screening based on the site on which the order was placed.

1. Go to the **Site Mapping** tab:



2. For each of your Kibo sites, enter the exact name of the corresponding site in Kount. The naming is case-sensitive.

   > To avoid errors, Kibo recommends copying the site name from within the Kount application and pasting it in the Site Mapping configuration.

3. Click **Save**.

Add the Kount Widget to Your Theme

The Kount Application includes a theme widget that is available on GitHub.

> The Mozu/Integration-KountWidget repository is private. Contact with your GitHub username to request access to this repo.

You can add this widget to the checkout page of your Kibo site(s) to capture customers' browser information for inclusion in Kount's fraud screening.

Update Your Theme

1. Clone or download the GitHub repository.
2. Add or merge the widget files, which are listed in the theme readme on GitHub.
3. Run Grunt to build the theme.
4. Upload the resulting ZIP file to Dev Center.

5. Install the updated theme to the sandbox you're working in.
6. In Admin, go to **Main** > **Content** > **Themes** to apply the new theme.

Add the Widget to Your Checkout Page

Note that you can only perform this step if you are using a Kibo site.

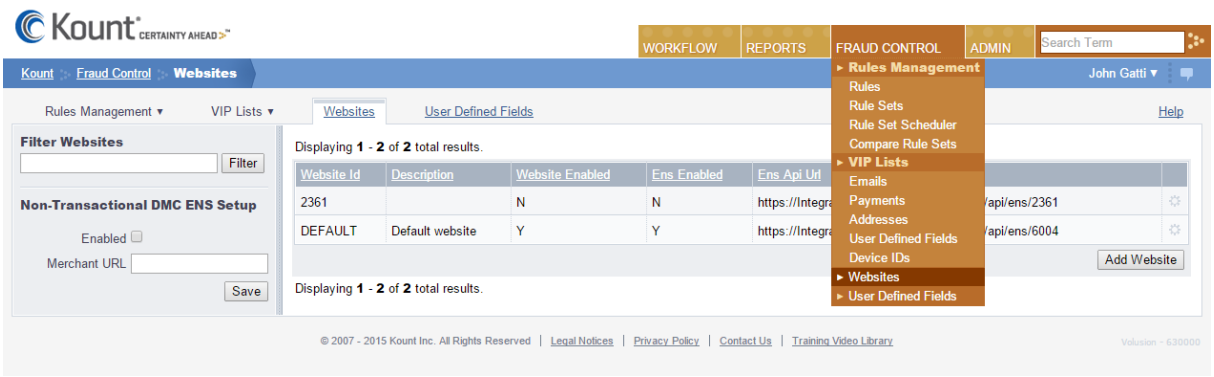
1. In Admin, go to **Main** > **Content** > **Editor**.
2. In the **Pages** view of the site tree, navigate to **Templates** > **Checkout**.
3. Switch to the **Widgets** view of the site tree.
4. Drag the **Kount Fraud Detection** widget to any dropzone on the checkout page. The widget is not visible to customers, so placement on the page is not important.

Enable the Kount Event Notification System

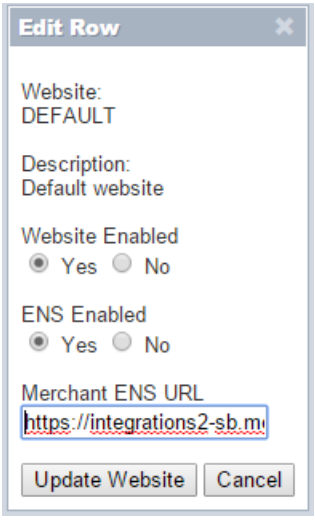
The Kount Event Notification System (ENS) enables third-parties such as Kibo to receive notifications when certain status changes occur in Kount. For example, you can review and approve an order within Kount, add history content, and update addresses. ENS syncs this data back into Kibo within a minute of the change occurring. ENS can sync the following changes back to Kibo from Kount: Edits to order content, history, shipping and billing addresses, and state changes such as from `Review` (R) to `Approve` (A).

> If you simply want to send orders to Kount and receive fraud detection results, you do not need to complete this section. However, if you do not enable the Kount ENS, any orders that Kount marks `review` (R) will remain in Pending Review in eCommerce regardless of whether you later accept the order in Kount.

1. Open the Kount Application configuration dialog, go to the **Account Settings** tab and copy your **Merchant ENS URL**.
2. Log in to Kount.
3. In your Kount dashboard, go to **Fraud Control** > **Websites**.



4. You will have a "DEFAULT" website available in the list. Click the gear icon and select **Edit** to edit the site settings.
5. Set **Website Enabled** and **ENS Enabled** to **Yes**:



6. For the **Merchant ENS URL**, paste the URL you copied from the Kount Application.
7. Click **Update Website**.

Enable the Kount Application by Kibo eCommerce

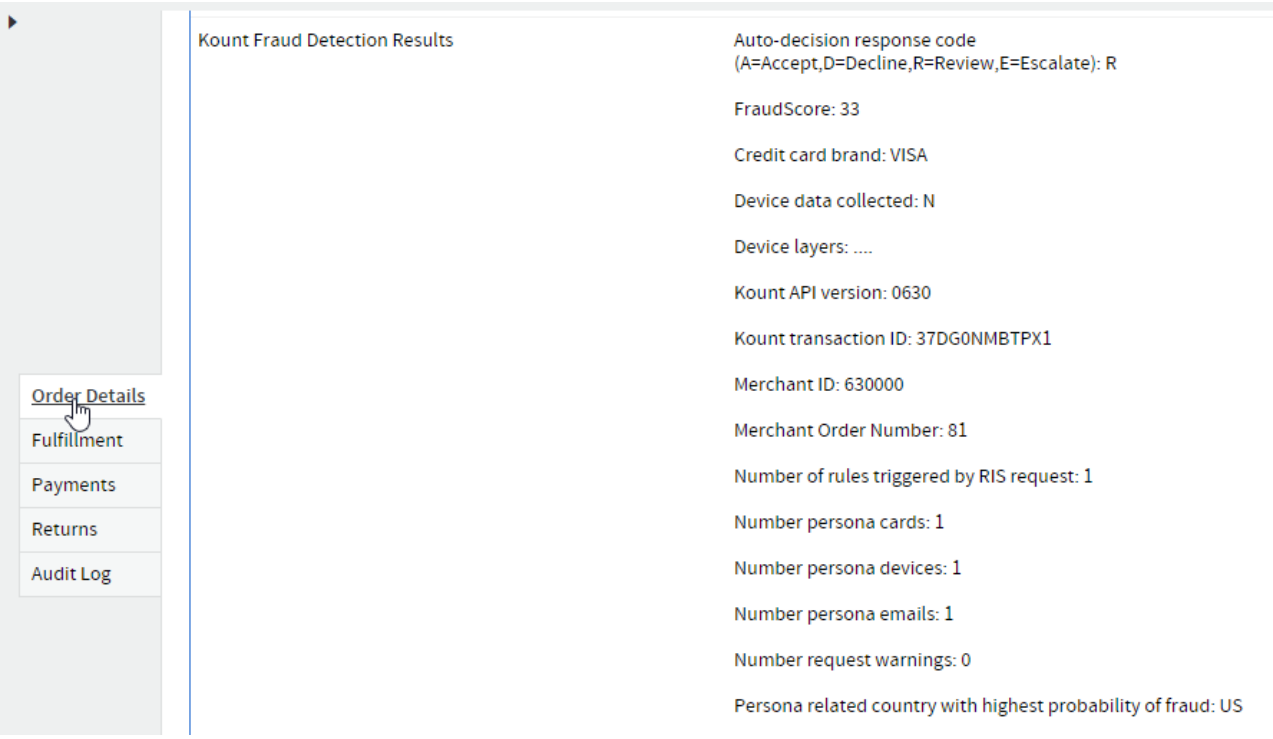
After configuration, enable the Kount application to apply its functionality to your tenant:

1. In Admin, go to **System** > **Customization** > **Applications**.
2. Click **Kount**.
3. Click **Enable App** on the Kount page.

Use the App

Once you have configured and enabled the Kount Application, the app automatically begins sending Kibo orders to Kount for fraud detection. When a Kibo order is sent to Kount, the status of the order in Kibo changes to **Pending Review**. Kount screens the order and attaches one of the following validation results: `Accept` (A), `Decline` (D), `Review` (R), or `Escalate` (E).

The result of the fraud detection appears in the **Order Details** in eCommerce:



Process Orders

When you process an order in Kibo, the Kount Application automatically updates the order status in Kount. If you have enabled the Kount Event Notification System, updates in Kount also propagate back to eCommerce. Order status maps between the two systems as follows:

Status Mapping: Kibo eCommerce to Kount

The following table describes how changes you make to an order in Kibo affect the order status in Kount.

Kibo eCommerce Status	Kount Status
Accepted	review (R)
Pending Review	review (R)
Completed	accept (A)
Cancelled	decline (D)

Status Mapping: Kount to Kibo eCommerce

The only Kount status change that Kibo captures is a move to `accept` (A). Any other status changes made in Kount leave the Kibo order in Pending Review so you can decide how best to process the order.

You must enable the Kount Event Notification System for Kibo to receive notifications of status changes after the initial fraud check.

Kount Status	Kibo Status
accept (A)	Accepted
review (R)	Pending Review
escalate (E)	Pending Review
decline (D)	Pending Review

AVS/CVV2 Mappings

When available, the Kount App sends the following credit card details to Kount to facilitate a more thorough fraud check:

- CVV2 number
- AVS zip code
- AVS street address

Most AVS and CVV (or CVN) response codes are standard across the online payment companies. However, the mapping of a specific response code from a payment gateway to the Kount AVS/CVV fields may vary depending on the payment gateway you use.

Standard AVS Response Codes

Refer to the documentation for your payment gateway for codes not in this list.

Code	Description
A	Street address matches. 5-digit AND 9-digit postal codes do not match.
B	Street address matches. Postal code could not be verified. (Non-US Visa cards)
C	Street address AND postal code do not match. (Non-US Visa cards)
D	Street address AND postal code match. (Non-US Visa cards)
E	AVS data invalid or AVS not allowed for this card type.
F	Card member name does not match, but postal code matches. (AMEX only)
G	Card issued by a non-US bank that does not support AVS.

Code	Description
H	Card member name does not match, but street address AND postal code match. (AMEX only)
I	Address could not be verified. (Non-US Visa cards)
J	Card member name, street address, and postal code all match. (AMEX only)
K	Card member name matches, but street address and postal code do NOT match. (AMEX only)
L	Card member name and postal code match, but street address does NOT match. (AMEX only)
M	Street address AND postal code match. (Non-US Visa cards)
N	Street address and postal code do NOT match.
O	Card member name and street address match, but postal code does NOT match. (AMEX only)
P	Postal code matches, but street address could not be verified. (Non-US Visa cards)
Q	Card member name, street address, and postal code all match. (AMEX only)
R	System unavailable.
S	US issuing bank does not support AVS.
T	Street address matches, but card member name does NOT match. (AMEX only)
U	Address information unavailable. Returned if if the AVS in a US issuing bank is not functioning, or if a US issuing bank does not support non-US AVS.
V	Card member name, street address, and postal code all match. (AMEX only)
W	9-digit postal code matches, but street address does NOT match.
X	Street address AND 9-digit postal code match.
Y	Street address AND 5-digit postal code match.
Z	5-digit postal code matches, but street address does NOT match.

Standard CVV Response Codes

Refer to the documentation for your payment gateway for codes not in this list.

Code	Description
M	CVV code entered matches the code on the card.
N	CVV code entered does NOT match the code on the card.
P	CVV code not processed.
S	Customer did not enter CVV code, but CVV code was expected.
U	Issuing bank not certified.

Mappings by Payment Gateway

The following tables describe how Kibo maps specific response codes from some of the most common gateways to Kount.

- Authorize.Net
- Cybersource
- Verisign
- CardConnect

Authorize.Net

Kount Mapping	M (Match)	N (No Match)	X (Not Supported)
AVS Street Address	X, Y	A, B, N, W, Z	C, D, E, F, G, H, I, J, K, L, M, O, P, Q, R, S, T, U, V
AVS Zip Code	X, Y	A, B, N, W, Z	C, D, E, F, G, H, I, J, K, L, M, O, P, Q, R, S, T, U, V
CVV2 Number	M	N	P, S, U

Cybersource

Kount Mapping	M (Match)	N (No Match)	X (Not Supported)
AVS Street Address	A, B, D, F, M, X, Y, 3	C, E, N, P, W, Z, 4, 5	G, H, I, J, K, L, O, Q, R, S, T, U, V

Kount Mapping	M (Match)	N (No Match)	X (Not Supported)
AVS Zip Code	A, B, D, F, M, X, Y, 3	C, E, N, P, Z, 4, 5	G, H, I, J, K, L, O, Q, R, S, T, U, V, W
CVV2 Number	M	• D— Issuing bank determined the transaction is suspicious. • I —CVV/CVN failed the processor's data validation. • N —CVV/CVN entered did not match the CVV expected.	P, S, U

Verisign

Kount Mapping	M (Match)	N (No Match)	X (Not Supported)
AVS Street Address	A, B, D, F, M, X, Y, 0	C, E, N, 1, 2	G, H, I, J, K, L, O, P, Q, R, S, T, U, V, W, Z
AVS Zip Code	D, F, M, X, Y, W, Z, 0	C, E, N, P, 1, 2	A, B, G, H, I, J, K, L, O, P, Q, R, S, T, U, V
CVV2 Number	M, Y	N	P, S, U

CardConnect

Kount Mapping	M (Match)	N (No Match)	X (Not Supported)
AVS Street Address	X, Y, W, Z	N	A, B, C, D, E, F, G, H, I, J, K, L, M, O, P, Q, R, S, T, U, V
AVS Zip Code	X, Y, W, Z	N	A, B, C, D, E, F, G, H, I, J, K, L, M, O, P, Q, R, S, T, U, V
CVV2 Number	M, P	N	S, U