

Stripe Payment Security: Understanding AVS and CVV Checks

Last Modified on 15/07/2025 1:33 pm IST

Stripe has robust security measures in place to effectively prevent fraudulent activities, including tools like CVV and AVS verification to authenticate cardholder information during online transactions.

What is CVV?

The CVV (Card Verification Value) is a three- or four-digit number printed on a credit or debit card, typically located on the back near the signature strip or on the front. It verifies that the customer has physical access to the card, adding a critical layer of protection against unauthorized use.

What is AVS?

The Address Verification System (AVS) checks whether the billing address provided by the customer matches the one on file with the card issuer. It's particularly useful for detecting suspicious activity in card-not-present environments like e-commerce.

AVS validates two key details:

- **Address Line Check**
- **Zip Code Check**

Each returns a result of "pass", "fail", "unchecked", or "unavailable". While "pass" and "fail" are the most relevant, not all banks support AVS, which may result in "unchecked" or "unavailable" statuses.

AVS Modes:

- **Non-strict AVS:** The transaction is reversed only if **either the Address or Zip Check** returns **"fail"**. All other combinations ("pass", "unchecked", or "unavailable") are accepted.
- **Strict AVS:** The transaction is reversed unless **both Address and Zip Checks** return **"pass"**. Any other result, including "fail", "unchecked", or "unavailable", will fail the AVS and trigger a refund.

If Stripe returns a **fail** for the Zip Check, the transaction fails the AVS and is refunded—even in non-strict mode.

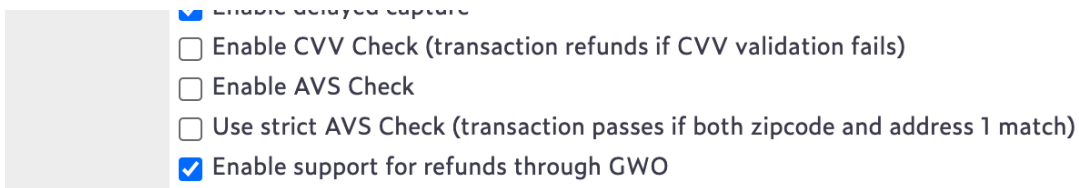
If you're only concerned with Address Line checks, you can configure custom rules within Stripe's dashboard to block transactions based on address results. In this case, you can disable AVS checks within WSM and rely entirely on Stripe's Radar rule engine. More info is available in [Stripe's documentation](#).

How to Enable AVS and CVV Checks on Your Platform

Steps:

1. **Log in to WSM.**

2. Navigate to **Orders > Payment Processor Setup**.
3. Click on **Configure Stripe**.
4. Under the configuration settings, enable the following options:
 - **Enable AVS Check** – This rejects transactions where the address or zip code validation fails.
 - **Enable CVV Check** – This refunds transactions if CVV verification fails.
5. Scroll down and **save your changes**.

A screenshot of the Stripe configuration settings interface. It shows a list of checkboxes for enabling various payment verification features. The first checkbox, 'Enable delayed capture', is checked with a blue checkmark. The other three checkboxes, 'Enable CVV Check (transaction refunds if CVV validation fails)', 'Enable AVS Check', and 'Use strict AVS Check (transaction passes if both zipcode and address 1 match)', are currently unchecked. The last checkbox, 'Enable support for refunds through GWO', is checked with a blue checkmark.

- ☒ Enable delayed capture
- ☐ Enable CVV Check (transaction refunds if CVV validation fails)
- ☐ Enable AVS Check
- ☐ Use strict AVS Check (transaction passes if both zipcode and address 1 match)
- ☒ Enable support for refunds through GWO

We strongly recommend placing a test transaction in an incognito window after making these changes to ensure the checkout process is working as expected.

You can read more about Stripe verifications and checks here:

<https://docs.stripe.com/disputes/prevention/verification>
