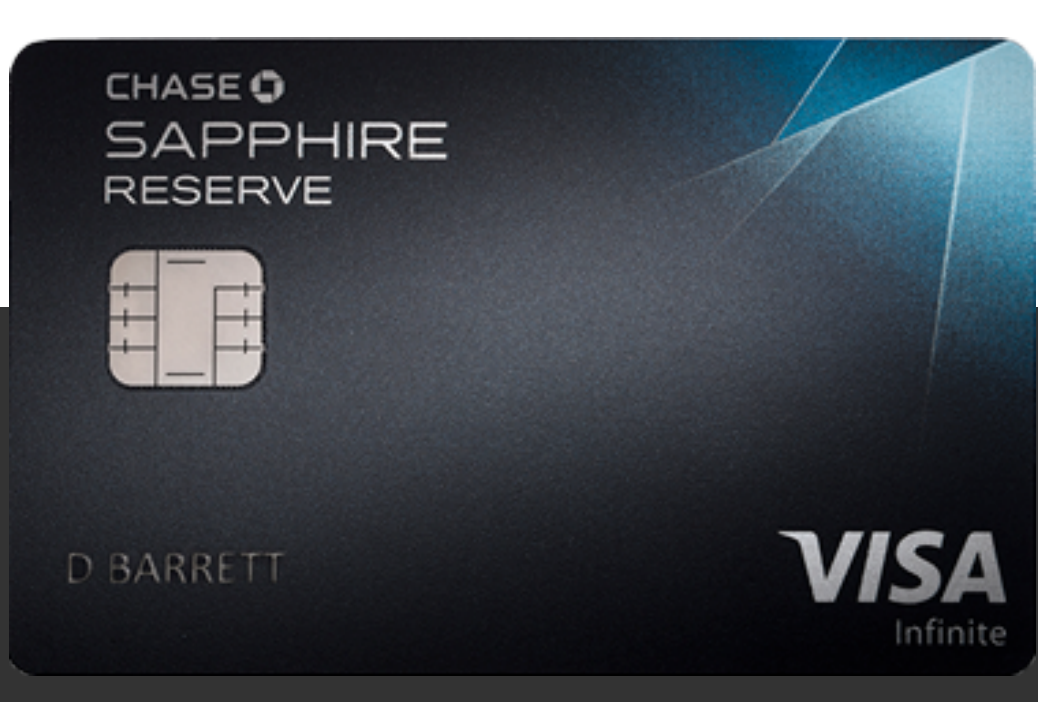
5 Best Practices for AVS



If your business regularly processes online transactions, it's important to have a set of rules in place to **help reduce** fraud **and** build customer trust. By following these AVS best practices, you'll be able to make better decisions for your business, and defend yourself when **fraud** does occur.

Understanding the ins and outs of AVS

Address Verification Service (AVS), is one of the most widely used practices in helping reduce fraud and protecting both you and your customer. The automated system is a way to verify a person's identity when they are not present at the time of transaction.

AVS will compare the billing address used in a credit card transaction against the information the bank has on file. The bank will return a corresponding response code indicating how closely the addresses match. If the addresses don't match at all, the transaction will likely be declined. However, you're able to customize your decision whether to complete or decline the card based on the response code and your own set of best practices.

AVS response codes: what does it all mean?

Some common responses:

A&W — Partial Match
Either the street addresses or zip codes don't match.

X&Y — Full Match
Both the street addresses and zip codes match what the bank has on file.

N — No Match
Neither the street addresses or the zip codes match.

R — Retry
System unavailable - run it again.

Your bank will return a letter response which corresponds to how closely the address used matches the address on file. These codes can help you determine whether to accept or decline a transaction.

01

Always be sure your payment gateway has AVS.

AVS is the first line of defense against fraud.

What the process looks like.

- The customer fills out the payment form with their billing address.
- The transaction is sent for authorization with the customer's credit card provider.
- Your online payment processor then cross-checks that address with the address on file.
- The issuing bank returns a response code indicating a full match, partial match, no match, retry, etc.

02

Don't rely solely on the bank's response codes.

Use the codes along with your own discretion when accepting a payment.

AVS is not a black or white system, as not every "partial match" or "no match" is a 100% guarentee of fraud. While automatically rejecting risky transactions will likely result in less fraud, the likelihood of lost revenue and the potential loss of business is far greater. At the same time, being too lax can leave you vulnerable to fraud and chargebacks.

If you're in the position to dedicate resources to evaluating these risky transactions before automatically declining them, you can make better decisions in the long run.

Common explanations for error codes other than fraud:

- A college student who uses their parents' credit card, but enters their dorm address.
- A buyer who has multiple credit cards, and doesn't remember which address is associated with which card.
- Someone just moved and their old address is still listed as their billing address, but they enter their new address.

03

AVS does not prevent chargebacks or fraud.

There are still ways for fraudsters to get around AVS.

Keep in mind:

- If the fraudster has access to the address associated with the credit card, AVS won't protect you.
- Many credit cards issued outside of the US, Canada, and the UK don't support AVS.
- You may still be liable for chargebacks if you can't prove you have layers of measures in place to prevent fraud - not just AVS.
- Since AVS only looks at numeric values, if a customer includes an address like "5th Street", it could confuse the system.
- AVS can work against you as much as it works for you. Allowing automatic declines based on the banks response can lead to significant revenue loss.
- Pre-paid cards will almost always fail an AVS check.

04

"No match" codes are the best indicator of fraud.

What to do when this occurs?

- Before declining the payment, first let the customer try again, but restrict the number of declined transactions they are allowed.
- Be prepared to reach out to the customer directly after multiple failed attempts.
- Have an automated email response set up to verify their identity and finances.
- While you shouldn't automatically reject a no match response, it's important to keep in mind that the risk of fraud goes up without an AVS match, and typically, so does the card's processing fee.

05

Implement different layers of protection.

AVS is just one piece of fraud protection.

- Keep records of all the processes you use to reduce fraud. If you can't prove you're actively protecting your customers, that's an automatic loss.
- Make sure your systems and services are PCI compliant.
- Always authenticate the customer's card and track the IP address where the payment is coming from.
- Be careful of vendors promising to eliminate fraud entirely - this is a false claim.
- Analyze individual behavior to determine what's normal/abnormal behavior for this customer.
- Enable a CVV (the three digits on the back of the card) filter to further help reduce fraud.

In the end, AVS can only help reduce the risk of fraud, but it's by no means a comprehensive solution, nor should it be the only method of fraud prevention you rely on to protect you and your customers. It can often be difficult to determine which technique will be best in deterring fraud, so the more layers of defense you have, the better. AVS is not a stand-alone solution. It's up to you to develop a system to fight fraud at every step.

As summarized by chargebacks911, Tidal Commerce, and Riskified.