Keep records of all the processes you go through to reduce fraud. If someone just moved and their old address is still listed as their billing address, but they enter their new address, it's an automatic loss. AVS can work against you as much as it works for you. If the fraudster has access to the payment gateway has AVS, AVS won't protect you. A college student who uses their parents' credit card, but enters their dorm address, will return a corresponding response code indicating how closely the address used matches the address on file. The bank will return a corresponding response code indicating how closely the address used matches the address on file. These codes are either a full match, partial match, no match, or a no-match retry. A&M X&Y does this all mean?

Always be sure your payment gateway has AVS. If your business regularly processes online transactions before automatically declining them, you can make better decisions in the long run.

Don't rely solely on the bank's response codes. Common explanations for error codes other than fraud:

- **What the process looks like:**
  - The customer fills out the payment form with their customer's credit card.
  - The transaction is sent for authorization with the provider.
  - The issuing bank returns a corresponding response code indicating how closely the address used matches the address on file. The transaction will likely be declined. However, you're able to customize your decision whether to accept or decline a transaction.
  - Before declining the payment, first analyze individual behavior to determine what's normal/abnormal behavior for this customer.
  - If you're in the position to dedicate resources to evaluating these risky transactions, doing so 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.

ASV does not prevent chargebacks or fraud. What to do when this occurs?

Implement different layers of protection.

"No match" codes are the best indicator of fraud. Implement different layers of protection and defend yourself when you have layers of defense you have, the better.

ASV response codes: what does it all mean?

- **Partial Match:**
  - Either the street addresses or the zip codes match. If the addresses don't match at all, the transaction is likely to be declined. However, you're able to customize your decision whether to accept or decline a transaction.

- **Full Match:**
  - Both the street addresses and zip codes match. If a customer includes an address like "5th Street", it could confuse the system.

- **No Match:**
  - Neither the street addresses nor the zip codes match.
  - "No match" codes are the best indicator of fraud. While automatically rejecting a no match response, it's important to keep in mind that the risk of fraud goes up without an AVS response code. If you can't restrict the number of declined failed attempts, let the customer try again, but before declining the payment, first analyze individual behavior to determine what's normal/abnormal behavior for this customer.

- **No Match Retry:**
  - The customer fills out the payment form with their customer's credit card.
  - The transaction is sent for authorization with the provider.
  - The issuing bank returns a corresponding response code indicating how closely the address used matches the address on file. These codes are either a full match, partial match, no match, or a no-match retry. A&M X&Y does this all mean?

- **What the process looks like:**
  - The customer fills out the payment form with their customer's credit card.
  - The transaction is sent for authorization with the provider.
  - The issuing bank returns a corresponding response code indicating how closely the address used matches the address on file. These codes are either a full match, partial match, no match, or a no-match retry.

- **Always be sure your payment gateway has AVS.** If your business regularly processes online transactions before automatically declining them, you can make better decisions in the long run.

- **Don't rely solely on the bank's response codes.** Common explanations for error codes other than fraud:

- **Partial Match:**
  - Either the street addresses or the zip codes match. If the addresses don't match at all, the transaction is likely to be declined. However, you're able to customize your decision whether to accept or decline a transaction.

- **Full Match:**
  - Both the street addresses and zip codes match. If a customer includes an address like "5th Street", it could confuse the system.

- **No Match:**
  - Neither the street addresses nor the zip codes match.
  - "No match" codes are the best indicator of fraud. While automatically rejecting a no match response, it's important to keep in mind that the risk of fraud goes up without an AVS response code. If you can't restrict the number of declined failed attempts, let the customer try again, but before declining the payment, first analyze individual behavior to determine what's normal/abnormal behavior for this customer.

- **No Match Retry:**
  - The customer fills out the payment form with their customer's credit card.
  - The transaction is sent for authorization with the provider.
  - The issuing bank returns a corresponding response code indicating how closely the address used matches the address on file. These codes are either a full match, partial match, no match, or a no-match retry.

As summarized by chargebacks911, Tidal Commerce, and Riskified, implementing different layers of protection is key to reducing fraud and protecting both you and your customers. It can often be more layers of defense you have, the better.