Address Verification Service (AVS)

Definition/Description

AVS allows CNP merchants to check the cardholder billing address with card Issuer. The merchant includes the AVS request as part of the authorization.

Applicability

Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-app [merchant app]	Yes	Customer onboarding	Yes	Merchants	Yes: internal
Mobile browser	Yes	Authentication (onboarding)	Yes	Issuers	Yes: internal
Desktop/laptop computer	Yes	Authentication (transaction)	Yes	Issuer processors	Yes: for clients
Phone	Yes	Authorization	Yes	Wallet/online payment providers	Yes: for clients
		Post-authorization review	Yes	Acquirer processors	Yes: for clients

Technical Features/How the Technique Works

A merchant can use AVS during checkout to verify the customer's billing address and/or zip code against the information on file at the issuer.

AVS can be used as a pre-authorization step known as an 'address verification,' or the AVS request can be embedded in the authorization request to the issuer.

The issuer responds with either a full match, partial match, or no match. If it is part of an authorization request, the issuer will embed the AVS response within the approval or decline message.

The merchant may use the AVS response to augment the response from the issuer. Most typically, a merchant may choose to decline a transaction, even if the issuer approves the transaction, if the AVS check returns a 'no match.'

Risks Associated with Technique

AVS typically would be used as part of a layered fraud solution. Fraudsters often have access to the cardholder's address information along with the stolen card credentials, so an AVS match alone should not be accepted as proof of a legitimate transaction.

False positives are a risk. Since AVS requires matching numerical fields in an address, which is often in a non-structured format, false declines are a possibility.

Customer Impact/Level of Friction

The process requires that the customer enter billing information when checking out or when establishing an account with the merchant. The customer needs to be aware of the address on file with the issuer and ensure it is up to date.

Implementation Considerations

Billing information is standard KYC information and capturing it is relatively easy.

Integration is not complicated. Using AVS is a common practice and is incorporated in the existing authorization message infrastructure.

AVS requires a low level of investment and provides a low level of protection. The technique is a standard part of typical CNP risk management and is used as part of a layered approach.

Maturity

AVS has been in use for many years and is a standard tool for addressing CNP fraud risk.

Applicable Industry Standards

Specifications for AVS vary by payment network.

Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

Further Reading

https://www.signifyd.com/resources/fraud-101/detection/avs-how-it-works/

https://www.verifi.com/kb/what-is-address-verification-service-avs/

https://www.vantiv.com/vantage-point/safer-payments/address-verification-service

Source Document: This technique is extracted from the *Card-Not-Present (CNP) Fraud Mitigation Techniques* white paper. That white paper was developed to provide a high-level document that directs readers to relevant fraud mitigation techniques while providing easy access to details about the solutions. The white paper is available at: https://www.uspaymentsforum.org/card-not-present-cnp-fraud-mitigation-techniques/

which requirements may change over time. The U.S. Payments Forum assumes no responsibility to support, maintain or update the Information, regardless of any such change. Use of or reliance on the Information is at the user's sole risk, and users are strongly encouraged to consult with their respective payment networks, acquirers, processors, vendors and appropriately qualified technical and legal experts prior to all implementation decisions.