Static Card Security Code

Definition/Description

A card security code (CSC) is a security feature that is used with CNP transactions. The card security code is also known as card verification data (CVD), card verification number, card verification value (CVV), card verification value code, card verification code (CVC), verification code (V-code or V code), or signature panel code (SPC). Major payment networks use the following names:

- Visa: Card Verification Value 2 (CVV2)
- Mastercard: Card Validation Code 2 (CVC2)
- Discover: Card Identification Data (CID)
- American Express: Card Identification Number (CID)

The CSC is supplemental to the primary account number (PAN) that is embossed or printed on most cards, and is three or four digits depending on the payment network.

The CSC is printed on the card, and when used, provides an indication that the cardholder possesses the card at the time of transaction.

Applicability

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

Technical Features/How the Technique Works

The cardholder provides the CSC to the merchant at the time of the transaction. The CSC is sent to the issuing bank as part of the authorization request. The issuing bank uses the code in deciding whether to authorize the transaction.

Risks Associated with Technique

The technique is vulnerable to methods such as keylogging, where keyboard input is captured, and phishing, where the cardholder is tricked into providing the code to a fraudster.

Because the static CSC is printed on the card, if the card has been stolen or information on the card copied, whoever has access to that card can potentially make online purchases.

Customer Impact/Level of Friction

Requiring a CSC introduces some friction into the transaction since the customer must manually enter the code. Since the customer will also be entering the card number and expiration date, the additional effort is small. However, the CSC is not stored by the merchant, so cardholders will need to reenter it when checking out at merchants where other card data is on file.

Implementation Considerations

Static CSC implementation requires low effort. Because CSCs are widely used, they are a part of virtually all shopping carts.

Maturity

The CSC technique was originally developed in the UK as an 11-character alphanumeric code by Equifax employee Michael Stone in 1995.[1] The concept was adopted by the UK Association for Payment Clearing Services (APACS)[2] and streamlined to the three-digit code known today. MasterCard started issuing CVC2 numbers in 1997, and Visa issued them in the U.S. by 2001.[3]

Applicable Industry Standards

This technique has no applicable industry standards.

Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

Further Reading

https://en.wikipedia.org/wiki/Card_security_code

https://www.cvvnumber.com/cvv.html

https://chargebacks911.com/card-security-codes/

https://www.merchantmaverick.com/what-is-cvv2-cvv-checks/

https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/

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/

[1] https://en.wikipedia.org/wiki/Equifax

[2] https://en.wikipedia.org/wiki/Association_for_Payment_Clearing_Services

[3] https://en.wikipedia.org/wiki/Card_security_code

Please note: *The information and materials contained in this document ("Information") is provided solely for convenience and does not constitute legal or technical advice. All representations or warranties, express or implied, are expressly disclaimed, including without limitation, implied warranties of merchantability or fitness for a particular purpose and all warranties regarding accuracy, completeness, adequacy, results, title and non-infringement. All Information is limited to the scenarios, stakeholders and other matters specified, and should be considered in light of applicable laws, regulations, industry rules and requirements, facts, circumstances and other relevant factors. None of the Information should be interpreted or construed to require or promote the establishment of any solution, practice, configuration, rule, requirement or specification inconsistent with applicable legal requirements, any of 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.*