BLOG PAGE

Payments

Authentication vs. Authorization

VALERIE HARE | JUL 13, 2022

Quick Hits:

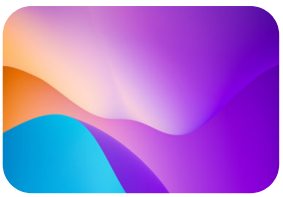
- Payment authentication is confirming an account or cardholder's identity.
- Payment authorization ensures that a cardholder has the appropriate funds or credit needed to fulfill a transaction amount.
- Merchants need to know the differences between authentication and authorization because these terms are often used interchangeably in the payment ecosystem.

What Is Payment Authentication?

Payment authentication verifies an account or cardholder's identity, such as for a one-time purchase or recurring subscription. While global commerce hit $4.2 trillion in 2020, the losses from fraudulent card purchases rose to $6.4 billion that same year. Indeed, authentication is a critical step to help prevent criminals from making fraudulent purchases with stolen debit and credit cards.

Payment Authentication Method

Since credit card fraud is a serious issue in today's payment landscape, a simple username and password are not enough to authenticate cardholders securely. Banks, card issuers, merchants, and payment processors use various factors to authenticate, which includes any of the following.



Want more content?

By subscribing to our mailing list, you will be enrolled to receive our latest blogs, product updates, industry news, and more!

Subscribe Now

- **What you know** – this is typically a username and password but can also be an answer to a security question or a one-time code that grants a user temporary access for a login session or transaction.
- **What you have** – this is usually a phone, app, computer, digital ID card, or security token.
- **What you are** – any biometric data, such as a fingerprint scan, facial recognition, or retinal scan.

Aside from simple security factors, financial institutions use various authentication methods to validate cardholders, such as CVV, AVS, CHAP, and 3DS. These tools are used to communicate with different parties, including banks, cardholders, card issuers, merchants, and payment processors, who work together to validate transactions.

Card Verification Value (CVV)

CVV is considered a standard authentication method for online transactions. Most merchants require the cardholder to enter the CVV code when making card-not-present (CNP) transactions. Cardholders can find this 3 or 4-digit code on the front or back of their credit or debit card. Requiring CVV codes can help prevent merchants from processing online transactions without valid codes. However, this method is only effective if combined with other authentication methods because cybercriminals can still make fraudulent purchases if they acquire a physical card with the CVV code.

Address Verification System (AVS)

AVS is designed to help prevent card fraud by comparing a card's billing address with the one the customer provided. When the address is provided, it's scanned to determine its accuracy based on the address stored on file via the credit card company. Depending on the accuracy level, the card issuer can issue a full, partial, or no AVS match. Merchants can use the AVS match results to approve, cancel, or manually investigate the pending transaction.

Indeed, it may be possible that a customer moved and did not update their card's billing address. However, fraudsters may also bypass the AVS by conducting an online search to identify the cardholder's address. Thus, while AVS is quick and easy to implement, it's not a standalone method because fraudsters can still bypass it by finding a person's address via social media or other resources.

Challenge-Handshake Authentication Protocol (CHAP)

CHAP checks a cardholder's identity by presenting a challenging question during the authentication process. If the person answers the question correctly according to the CHAP server's expected response, then the CHAP authentication is successful.

It's important to note that this method occurs before login, which means that the system doesn't use shared secrets to validate a person's identity. This protocol can help prevent replay attacks, which occur when a threat actor reuses stolen credentials.

CHAP is frequently used with Password Authentication Protocol (PAP) and is used before the user enters their password. A CHAP request can include a series of security questions or a small puzzle, which the user must complete to achieve authentication. Like other methods, CHAP doesn't provide enough authentication, so it's best to use it in conjunction with other methods. Furthermore, cybercriminals can guess CHAP challenge requests through social engineering.

3-D Secure (3DS)

3DS is a global standard used to authenticate cardholders making card-not-present transactions. This standard enables merchants and payment providers to transmit payment and authentication data to card brand companies to determine the risk of transactions. When verifying a cardholder's identity, these card brands will consider various information, including the billing address, geolocation, device ID, and transaction amount and history. Based on a transaction's risk level, the cardholder's bank can send authentication response codes to help authenticate a transaction.

If there is sufficient data to authenticate a cardholder, then the transaction is successful and can proceed through a frictionless payment flow. However, if a bank views a transaction as suspicious, the cardholder must complete a challenge request. This challenge step requires a cardholder to verify their identity via email, phone, or text. Once the challenge is completed, the transaction can continue to the next steps. This method is called risk-based authentication, as transactions are handled based on risk levels.

3-D Secure is a useful authentication tool that can help reduce cart abandonment, check-out times, and chargebacks, as well as help, prevent payment fraud. Unlike other methods mentioned above, 3DS uses numerous data points to verify a cardholder's identity, uses machine learning to identify fraudulent activity, and is consistent with industry best practices for authenticating cardholders.

Discover 3-D Secure

What Is Multi-Factor Authentication?

Multi-factor authentication (MFA) requires users to provide two or more verification factors to gain access to a resource, such as an app or an online account. For example, a financial website may require users to enter their username and password and submit a one-time code sent via text, or provide a fingerprint scan. Indeed, this authentication method is crucial for an organization's identity and access management (IAM) policy. By using more than just a single security layer, MFA can help prevent threat actors from gaining access to and stealing a person's sensitive payment and personal data.

What Is Payment Authorization?

Payment authorization verifies that a credit or debit card is valid and contains sufficient funds to cover a pending transaction. This step always follows authentication and is necessary to approve a transaction. Unlike authentication, authorization is neither seen nor changed by the customer. This method is designed to grant or deny access to resources, such as approving or denying a credit card purchase due to a lack of available funds.

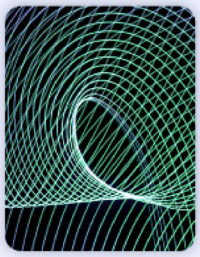
For an online purchase, a hold may be placed on approved funds. The customer's bank account will have a pending transaction during this holding period. Once the product ships, those funds are captured via the merchant's account.

Payment Authorization Methods

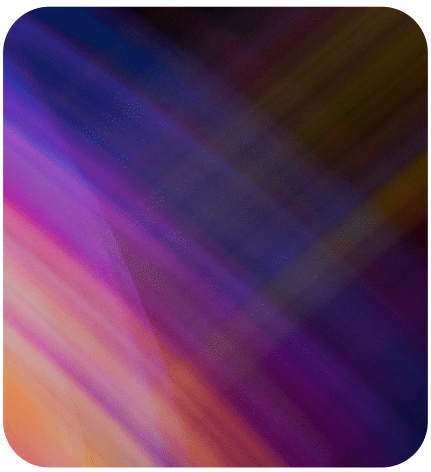
When a credit or debit card transaction is processed, the card issuer will send the authentication details (response codes) to the merchant's acquiring bank. These authorization codes, which vary for each card brand, payment processor, or gateway, usually contain two digits (like 00) or a letter and number (N1). The acquiring bank will either approve or decline the pending transaction for the merchant, which depends on whether there are sufficient funds in the cardholder's account. A final authorization process is necessary for the merchant's bank to deposit the appropriate funds into the merchant's account. Further, authorization is essential when a cardholder's bank account is debited or a credit or debit card is charged for payment via the ACH network.

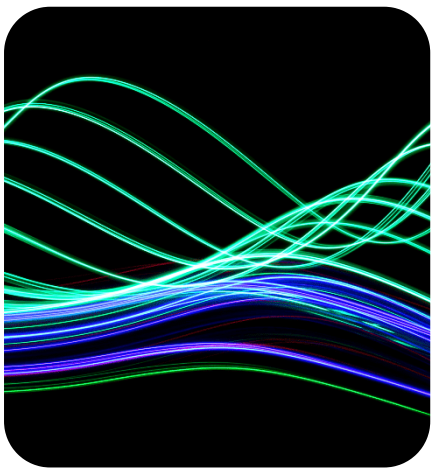
Payment Security Is a Must for Merchants

Aside from authentication and authorization, what else can businesses do to protect their customers' payment information? Payment tokenization is an effective solution with numerous advantages, including improving your data security, site checkout experience, and customer loyalty. Additionally, you can pass off the task of achieving and maintaining PCI compliance to the tokenization provider. If you are considering payment tokenization, contact TokenEx today to learn more about our payment tokenization designed to secure all your payment data. This includes primary account numbers (PANs), card verification values, automated clearing house transactions, and much more. Our expert cloud-based services work behind the scenes, so you can focus on growing your business and achieving your goals.



Choosing the right tokenization provider is critical. Read this to learn how we can help. →





NOV 30, 2023 Payments

Unlock the Full Potential of your Payment Data with TokenEx and acceptcards®

Owning your payment data is essential to fully unlock your payment stack and enable strategic payment processing. Learn more in this blog.

Read more

OCT 18, 2023 Payments

Making Payments Strategic: Three New Products for Card Lifecycle Management

Finding the perfect payment service provider, one with low rates and fees that offers every capability you need, is a thing of the past. For businesses looking to optimize their revenue, strategic payment processing has never been more crucial.

Read more

JUN 16, 2023 Payments

Why Account Updater Is Critical for Optimizing Revenue

Account updater is an easy-to-adopt tool that can increase customer satisfaction and company revenue. Learn more about how it works, and how you can increase successful transactions, in this blog.

Read more