3D Secure

3D Secure is a trusted protocol that connects digital merchants and financial institutions at the time of online checkout.

- Prevent fraud and unauthorized card use online.
- Choose from Zero Touch Authentication or One-Time Passcode Authentication.
- Improve member cardholder experience.
- Reduce risk of fraud.

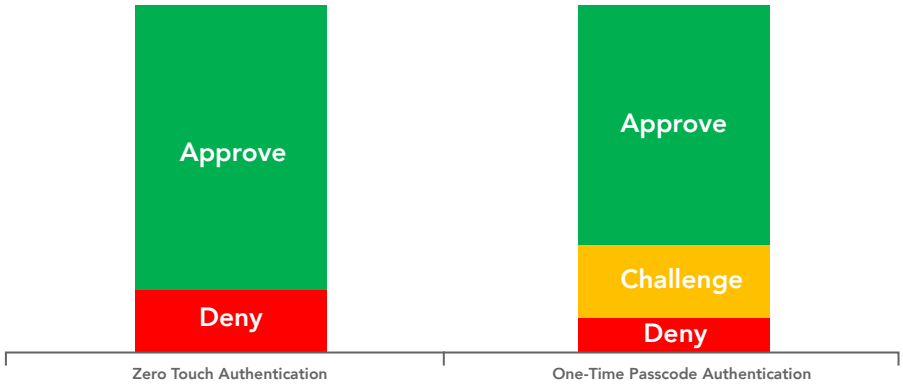
Digital transactions have become commonplace. With most cardholders completing transactions online, implementing strong, effective tools to prevent fraud and unauthorized card use has never been more important.

3D Secure, offered through our partnership with Fiserv, is a risk-based authentication solution. This secure protocol connects digital merchants and financial institutions at the time of online checkout. It is trusted and used by Visa, MasterCard, American Express, Discover, and more.

How It Works

3D Secure uses a variety of factors to authenticate a transaction. Outcomes at the time of authentication are determined by a scoring algorithm and a set of fraud strategies. Two risk mitigation components are built into 3D Secure: One-Time Passcode (OTP) and Zero Touch. The goal is to allow low-risk activity, challenge medium-risk activity via OTP, and deny high-risk activity via Zero Touch.

Authentication Methods



One-Time Passcode

With OTP, the cardholder's purchase is presented for authentication. It can be approved, denied, or challenged by OTP. A six-digit OTP is randomly generated when an authentication request is deemed a medium- to high-risk activity and engages Fiserv's Step-Up program. At that time, an SMS text message or an email is sent to the member to confirm the transaction in question. Once the member receives the OTP, they enter it into the dialog box on the merchant's checkout page. The OTP will then be verified to determine if authentication is successful or if it has failed. The user has 10 minutes from the time an OTP is sent out to use it before it expires.

3D Secure

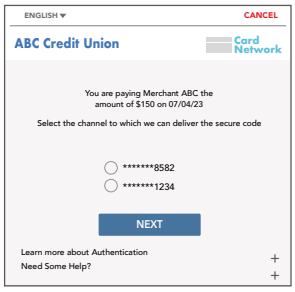
One-Time Passcode Experience

Low Risk: Silent Authentication

Authentication approved silently

(No screen displayed to user, no friction)

Medium Risk: Challenge



High Risk: Deny

Zero Touch

With Zero Touch, no challenge is presented to the cardholder and an ALLOW or DENY strategy is used based on set criteria. Authentication is dependent on the set predictive model risk score and fraud strategies. If denied, the cardholder can contact your credit union for assistance or exception processing. This is a frictionless approach with no cardholder interaction: The goal is to allow low-risk activity and deny high-risk activity.

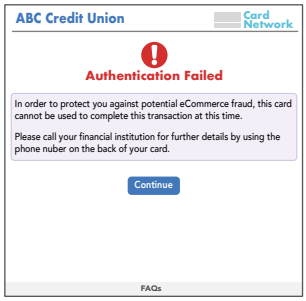
Zero Touch Experience

Low Risk: Silent Authentication

Authentication approved silently

(No screen displayed to user, no friction)

High Risk: Deny



Key Benefits

Minimize Fraudulent Card Use: Prevent fraud and unauthorized card use online.

Provide a Positive Member Experience: Use Zero Touch Authentication or One-Time Passcode Authentication to manage transactional risk.

Offer Control to Members: Offering email or SMS text notifications helps members be part of the process.

Reduce Staff Time: By automating many aspects of the authentication process, staff can focus on other areas.

"Striking the balance between convenience and preventing fraudulent card transactions can be tricky. 3D Secure is an automated solution that still allows a credit union to select its criteria for authentication. Members gain peace of mind knowing their credit union is being diligent and also have some control in how they opt to receive one-time passcodes when needed."

Rebekah Higgins
Chief Growth Officer

Learn More

For additional information about implementing 3D Secure at your credit union, please contact your dedicated Client Success Manager.