CO OP Solutions

FREQUENTLY ASKED QUESTIONS

EMV 3-D Secure One-Time Passcode (EMV 3DS)

What does it do?

What is EMV 3-D Secure (EMV 3DS) One-Time Passcode?

One-time passcode is an optional feature for the EMV 3DS product. This feature utilizes rules to require a member to receive a one-time passcode for certain card-not-present transactions that have exhibited heightened risk. This passcode helps verify a member's identity at the point of purchase and is a feature your cardholders expect. Many are already using it in everyday life.

What are the benefits of one-time passcode?

- It provides an additional layer of authentication for EMV 3DS transactions.
- It enhances the member experience while maintaining security by providing authentications with heightened risk a greater chance of being successful.
- It improves authorization rates securely: Authentications that relied only on using data elements now have a second method of being approved.

How is one-time passcode used in EMV 3DS?

The one-time passcode feature further verifies a member's identity as they perform transactions. All cardholding members will be auto-enrolled in the one-time passcode feature. EMV 3DS uses risk-based rules to authenticate members based on data elements provided during authentication. When the one-time passcode process is in effect, these rules may require a cardholder to receive a one-time passcode to successfully authenticate their transaction.

What is important to know before enabling one-time passcode?

One-time passcode will be added into the current rules for EMV 3DS. Once added, the authentication process will require member interaction when a one-time passcode process is required. A one-time passcode will be delivered to your members via SMS only when members are required to accept, receive and enter a one-time passcode for authentication completion. Credit unions need to provide Co-op with accurate member mobile number data in the accurate locations.

Members with incorrect or missing mobile data on file will receive failed authentications, which are a negative member experience. To ensure a positive member experience, credit unions should verify and update the mobile phone information on file for members in the designated fields. Members who receive failed authentications will likely need to call their credit union for resolution.

How does it work?

How does one-time passcode work?

The one-time passcode process includes the following three actions:

- **Creation** | As a member shops online and their purchase is determined to require a one-time passcode, the merchant's screen will ask the member to accept a one-time authentication process or close the transaction window. The intent is for the member to accept the one-time passcode request and initiate the authentication. If the member chooses to close the window, the authentication process will end and the merchant will guide the member through the next step.
- **Delivery** | The member selects the mobile number presented to them on screen and chooses to continue. Co-op then prepares the one-time passcode. Co-op verifies the member is allowing a one-time passcode to be provided, then initiates delivery of the one-time passcode to the member's selected mobile number.
- **Verification** | The member sees a screen for entering the one-time passcode on the merchant's site. When the passcode is entered, Co-op will verify that it was entered correctly. If the one-time passcode is successful, the member's authentication process is completed successfully and the merchant proceeds with the next step of the purchase process.

What is the SMS communication verbiage that the cardholder will see for a step up authentication for 3D Secure?

FreeMSg: CMS Alert DO NOT Share this code with anyone. We will never ask for this code. Your one-time passcode from Member CU is XXXXXX. Reply Stop to opt-out.

(CMS stands for Card Management System)

What number will the One-Time Passcode come from?

US-Domestic 44397

Canada TETFN +18888559935

(International) Alpha Code COOPOTP

What happens if the number is invalid on file?

The option to send to that number on file will still populate as an option for the cardholder.

What happens if the phone number on file that is populated is wrong?

Call holder can call in and have the new number updated.

Is there a grace period that a cardholder needs to wait for once the correct number is updated to receive an OTP?

Once updated, the new number should be applicable for One-Time Passcode.

What is the opt-in and/or opt-out process for members?

- **Automatic opt-In** | EMV 3DS rules govern all BINs for the credit union. When one-time passcode rules are included, all members are automatically "opted-in" to participate. Members will elect to receive one-time passcodes as part of the authentication process and for each authentication attempt. If a member does not accept the one-time passcode, their authentication will fail.

- **Opt-out (not recommended)** | The only way for a cardholding member to opt-out of the one-time passcode feature is to reply "STOP" using their mobile device. This is not recommended. If a member does this and continues shopping online, they will not receive one-time passcodes when required for subsequent purchases due to the opt-out they elected. The member will always receive a failed authentication for these transactions until they allow one-time passcodes again.
- **Opting back in** | Cardholding members who have replied "STOP" to a one-time passcode text can opt back in by texting the word "RESUME" to short code 44397.

What should a member do after receiving a failed one-time passcode authentication?

If a member receives a failed authentication, they will be instructed to contact the credit union for assistance. Credit union agents will perform the same identity checks they use today and can set the card number into bypass on the VCAS system, allowing the member to attempt the authentication again.

When members contact the credit union after a failed one-time passcode authentication, the credit union should further identify the member before taking action to bypass. Because one-time passcode is used for heightened-risk authentications, it's important to confirm the member's identity before making informational updates or setting the card in bypass.

Why would a member fail authentication for one-time passcode?

One-time passcode authentications will fail for various reasons. The most common reasons are:

- The member can't receive the one-time passcode because they don't have mobile data on file at Co-op.
- The member enters the one-time passcode incorrectly.
- The member has issues with their mobile provider. For example, their coverage may be spotty, making a one-time passcode undeliverable; the carrier might be having issues; or the member may have plan limitations.
    - In these cases Co-op can work with the credit union in a limited capacity to research an issue if it's raised within the required lead time.

What if a member exits the one-time passcode process flow?

The result is similar to the failed one-time passcode authentication process: The member willreceive a failed authentication and be instructed to contact the credit union as they would be without the one-time passcode function.

What if a member does not receive a one-time passcode?

The credit union should verify the member's mobile number data on file by ensuring it is located in the correct place in the Co-op cardholder file. If the data is deemed correct, contact Co-op at ClientCare@coop.org for further evaluation of issues in delivery.

Should I communicate anything about one-time passcodes to my members?

Yes. We highly recommend you manage member expectations by sending a communication prior to launching. Co-op has created some sample language you can use as is or update accordingly.

Do we need to add one-time passcode legal language on our website or in membership agreements?

- **Website** | Terms and Conditions will be provided to your credit union for inclusion on your website and must remain on your website as long as you are using the EMV 3DS One-Time Passcode.
- **Membership agreement** | You may consider adding something similar to the website Terms and Conditions in the membership agreement if your credit union deems it necessary to include it in multiple locations.

What is required to enable one-time passcode?

If applicable, Co-op Debit and/or Credit clients must be on AP Batch 4 to qualify. The AP Batch 4 setup ensures member mobile numbers can be provided to Co-op in the correct field on cardholder files.

Note that for any participating credit union, member mobile information must be verified and kept up to date by your credit union in order to ensure a consistent and positive member experience.

How do we implement one-time passcode?

Your Co-op onboarding team will help you and will provide a step-by-step process to guide you. We recommend the following items for implementation:

- **STEP 1 | Member mobile validation campaign**
  - Credit unions introducing one-time passcode into their rules sets for authentications may want to establish data validation campaigns with their members to verify that the data on file for mobile numbers is correct and in the correct field when passed to Co-op.
- **STEP 2 | Create a plan for failed one-time passcode authentications**
  - We recommend you complete additional member verification before setting failed one-time passcode cardholders for bypass or before updating member mobile information on file.
- **STEP 3 | Website Terms and Conditions**
  - Credit unions will want to add Terms and Conditions for EMV 3DS One-Time Passcode to their credit union websites in a place that's visible to their members. Co-op will provide this language.
- **STEP 4 | Member awareness**
  - We recommend sending a communication to your clients to manage their expectations. Co-op has created language for you to leverage and/or update for use with your members.

Can the credit union set a limit mandate for transactions over a $1,000 for one-time passcode?

Yes.

How does one-time passcode impact the authentication process?

Today, the EMV 3DS risk-based authentication process is completely seamless to your members. Adding one-time passcode introduces an added step in the authentication process for the member. However, members expect their credit unions to put the right protections in place and they are already using one-time passcodes in their daily lives. The process itself is simple: Members select their mobile number to receive a one-time passcode when prompted. In the case of failed authentication, they should contact their credit union directly for further support.

How do we recognize a one-time passcode in Visa Consumer Authentication Service (VCAS)?

All EMV 3DS One-Time Passcode authentications are logged in the VCAS application. A transaction from a member who has been authenticated in the past without a one-time passcode will show in this file as a "riskbased authentication," meaning this authentication was performed by using only the rules set by the credit union. Authentications that enact the one-time passcode process that VCAS field for the authentication method will display as OTP.

Can a credit union customize one-time passcode messages and/or specific portions of a message?

No. The one-time passcode messaging is static and the same for all credit unions.

How do we get started?

If I want to add one-time passcode, what do I need to do??

Contact your Client Business Executive or Client Business Manager who will walk you through a set of prerequisites and checklist items to make certain one-time passcode works for your credit union.

Who will manage my one-time passcode rules?

Co-op Fraud Teams will continue to manage your EMV 3DS rules and work with you to integrate the one-time passcode process into your rules. Co-op will continue to monitor your activity and rules, and may make suggestions for updates as fraud trends develop. Co-op highly recommends updating your rules to include one-time passcode. This offers yet another way to verify a transaction when current rules provide a failed authentication.

What are ECI Indicators?

ECI Codes are the values that are returned from the Directory Service, the ECI Codes indicate the result of the 3D Secure Transactions.

- **Visa ECI**
  - ECI = 5: This value means that the cardholder was authenticated by the issuer by verifying the cardholder's password or identity information. The value is returned by the ACS in the Payer Authentication Response message when the cardholder successfully passed 3-D Secure payment authentication.

- ECI = 6: This value means that the merchant attempted to authenticate the cardholder, but either the cardholder or issuer was not participating. The value should be returned by the ACS in the Authentication Response message for an Attempt Response. Additionally, merchants may use an ECI 6 in the authorization request when a Verify Enrollment of N is received from the Visa Directory Server.
- ECI = 7: This value is set by the merchant when the payment transaction was conducted over a secure channel (for example, SSL/TLS), but payment authentication was not performed, or when the issuer responded that authentication could not be performed. An ECI 7 applies when either the Verify Enrollment or the Payer Authentication Response contains a U for Unable to Authenticate.

- **Mastercard ECI**
  - ECI = 02 : This value means that the cardholder was successfully authenticated (SLI = 2)
  - ECI = 01 : This means that the authentication could not be completed but a proof of authentication attempt was provided SLI = 1.
  - ECI = 00: This value means that the 3DS authentication is either failed or could not be attempted; possible reasons being both card and Issuing Bank are not secured by 3DS, technical errors, or improper configuration.

How can I get more information?

Co-op is encouraging all clients to investigate the benefits of EMV 3DS risk-based authentication with support from Co-op. For more information, contact your Client Business Executive or Client Business Manager. You can also call (800) 782-9042, option 6 or email solutions@coop.org.

CO OP Solutions℠