TruStage™

Two-factor authentication

Risk overview

Two-factor authentication, also referred to as out-of-band authentication, is a layered security control for online banking that uses a separate communications channel to authenticate a member. It's considered a "must have" control to help mitigate the risk of account takeovers through online banking.

Two-Factor Authentication

Managing the risks of account takeovers via online banking requires a layered security program. The use of multifactor authentication alone for online banking is not sufficient to protect member accounts. Layered security controls are characterized as different controls at different points in the transaction process so that if one control is defeated, another one exists that could help prevent unauthorized transactions.

Two-factor authentication or out-of-band authentication typically leverages the use of one-time-passcodes (OTPs) and can be used in these cases:

- To authenticate a member attempting to login to their account using a device not recognized by the host system;
- To verify all transfers or those exceeding a monetary threshold that members initiate through online banking;
- To verify wire transfers requested via online banking;
- To verify changes to member contact information (e.g., changes to member's home and mobile phone numbers, mailing address, email address, etc.) made through online banking;
- To verify password changes initiated through online banking; and
- To verify password resets using the "forgot password" feature.

When a member attempts a transaction that triggers two-factor authentication, an OTP is generated and typically delivered to the member via automated phone call, email, or SMS text message.

Members have a choice in the delivery method using the contact information the credit union has on file. Upon receipt, the member must enter the OTP to continue with the transaction.

Educating members of scams and your use of OTPs is also important to successfully mitigate risks.

- Educate them to be wary of texts or calls appearing to come from the credit union. Advise members to call the credit union using a reliable phone number to question any text message or phone call purportedly received from the credit union.
- Inform members to never provide personal information in response to a text message or phone call purportedly from the credit union. Additionally, advise members that no credit union employee would ever ask for personal information, such as account numbers, usernames, passwords, and passcodes.

Risks associated with OTPs

Transmitting OTPs in SMS text messages continues to be a common delivery method. However, fraudsters' social engineering tactics allow them to hijack incoming calls and SMS text messages. In addition, security experts have warned that legitimate businesses offering SMS marketing and mass messaging can potentially be used by fraudsters to hijack SMS text messages.

- Fraudster social engineers call center into changing member's contact information, including home and mobile phone numbers and email addresses.
- Fraudsters social engineer members into providing OTPs to the fraudsters.[1]
- Email accounts can be hacked allowing a fraudster to intercept the OTP. In fact, some have experienced losses from account takeovers when fraudsters hacked member email accounts to intercept the OTPs. [refer to Account Takeover Fraud Case Study]
- Member mobile devices can be ported to a different carrier without the member's knowledge allowing the fraudster to receive calls and SMS text messages intended for the member.[1]
- Member could be a victim of SIM swapping where the fraudster social engineers the member's mobile phone carrier into activating a replacement SIM that the fraudster has in their possession.[1]
- Member mobile devices can be infected with malware that redirects SMS text messages to the fraudsters.

[1]Several of these tactics have been used in the Zelle fraud scam.

Account takeover fraud case study

- Credit union deploys two-factor authentication for the online banking enrollment feature on their website.
- Fraudster enrolled a member's account for online banking
- Fraudster hacked member's email account to intercept the OTP needed to complete online banking enrollment
- Once enrolled, the fraudster changed the member's contact information (home and mobile phone numbers and email)
- Fraudster requested three wire transfers totaling $312,000 via online banking
- Callback verifications were performed but they were made to the fraudster who answered the security questions

Zelle/Peer-to-Peer (P2P) fraud

The traditional Zelle/P2P fraud scam surfaced in 2019 with fraudsters sending text alerts to members appearing to come from the credit union warning members of suspicious debit card transactions.

This fraud scam continues with losses ranging from $30,000 up to $2.7 million.

Zelle appears to be targeted due to the speed in which the payments are made (minutes rather than hours or days); however, other vendor P2P products have also been targeted.

- The scam begins with fraudsters sending account alerts to members via text message – appearing to come from the credit union - warning them of suspicious debit card transactions on their accounts.
- The fraudsters call the members who respond to the text spoofing the credit union's phone number claiming to be from the credit union's fraud department and are calling to verify suspicious transactions on the member's account.
- To verify the identity of the member, the fraudster asks for their username and tells them they will receive a passcode via text message and the member must provide the passcode over the phone.
- The fraudsters attempt a transaction that triggers a two-factor authentication passcode, such as using the "forgot password" feature, and the passcode is sent to the member via text or email who, in turn, provides it to the fraudster.
- The fraudster immediately uses the passcode to login to the member's account, changes the online banking password, and uses Zelle / P2P to transfer funds to others.

The Zelle/peer-to-peer (P2P) fraud scam continues to impact members with losses ranging from $30,000 up to $2.7 million.

Source: Internal claims data, TruStage

Credit unions should avoid transmitting OTPs in emails due to the risk of hacking member email accounts. In fact, several account takeovers occur when fraudsters hack member email accounts to intercept the OTPs.

The National Institute of Standards and Technology (NIST) has also changed its position on using SMS text messages to deliver two-factor authentication passcodes due to its inherent insecurities. Instead, NIST recommends using a push-based two-factor authentication method that relies on pushing notifications to a dedicated app residing on users' mobile devices. Refer to NIST Special Publication 800-63B, Digital Identity Guidelines.

To effectively mitigate the risk in transmitting OTPs in emails and SMS text messages, credit unions should deploy a two-factor authentication solution that does not rely on transmitting OTPs via automated phone call, email, and SMS text message.

Effective two-factor authentication methods

- Push notifications to a dedicated app residing on the member's mobile device alerts the member of attempted logins. The member is given a choice to approve or deny the login attempt.
- Soft token residing on the member's mobile device generates an OTP that the member must enter to complete the login.

Looking for additional insights?

- Access the Business Protection Resource Center (User ID & Password required) for exclusive risk and compliance resources to assist with your loss control efforts.
- Go to Emerging Risks Outlook for critical questions, answers, and resources to help build additional awareness and drive organizational action.
- If you'd like to discuss this risk in more detail, simply schedule a no-cost 1:1 discussion with a TruStage™ Risk Consultant by contacting us at riskconsultant@trustage.com or at **800.637.2676**.

#10009640-0823 © 2023 TruStage

TruStage™