General Information

Question:	Answer:
Where can members change their password?	Passwords can be changed in online banking via desktop or mobile app. Passwords cannot be changed via Mobile Web.
What are the requirements for a new strong password?	8-30 characters 1 uppercase letter 1 lowercase letter 1 number Special characters are optional
What special characters can be used?	Optional special characters include @ # | $ - !
Will a strong password expire?	Yes, passwords will expire every 365 days.
Will members receive a warning message in online banking prior to their password expiring?	No, upon expiry the member will be prompted to change their password.
Can I reuse a previously used password?	The last 10 passwords **CANNOT** be reused.
Why is a generic error message presented when I haven't met the minimum requirements rather than reflecting the actual problem (ie, password is too short or too long)?	It is against the Payment Card Industry (PCI) compliance to expose the actual issue that is preventing the password from validating. It would be a security risk to advise the member that the password is too long, too short, doesn't contain the right mix of characters or is a password that has been used within a certain time frame. If hackers were trying to gain access to a member's online banking, they could use such information to discern what the password really should be.

Lockouts

| Question:	Answer:
Why am I locked out of Mobile App after updating to a strong password via desktop?	The user has likely enabled "**Quick View**" on their mobile app. This feature stores the password on the backend of all devices the member has ever had, allowing the app to retrieve balances and display them without the user having to login. Each time the app is opened and balances displayed, it's logging in with the previously stored password, which is incorrect. This will eventually lock the user out. To correct, the member needs to login to online banking via desktop. Navigate to 'Account Services' > 'Mobile Banking App' and remove all registered devices. Next the credit union will need to reset the lockout in the banking system. **If the member has changed to a strong password using their Mobile App, this will not be an issue.**
Why am I locked out on my desktop after updating to a strong password via desktop?	One reason for the lockout may be that the **old password** has been saved within the browser. If a password has been saved, it *will auto-populate* on the login screen. If the member does not re-enter the password prior to attempting to log in, they could inadvertently be logging in with the old saved password, eventually locking themselves out. To correct, the member needs to clear their saved passwords generally be deleting their cache/cookies in their browser settings. Next, the credit union will need to reset the lockout in the banking system. PLEASE NOTE: the member could also be locked out due to using Quick View on their Mobile App. See previous question.

MDSB Information

Question:	Answer:
Can a delegate login to Small Business Online Banking prior to the signer reactivating them?	No. If the delegate tries to login before they are reactivated, they will receive the Change Password screen. When they try to change their password, it is not accepted and the Change Password screen is simply provided again. Signers must update to strong password and reactivate delegates. See MDSB Delegate Management guide for details.
Is a delegate required to use a strong password?	No. 1. If the signer reactivates an existing delegate and does NOT assign a new temporary password, the delegate can continue to login using their original 5-8 digit numeric password. 2. If the signer assigns a new temporary password (for a new or existing delegate), the signer must create a temporary password that is **5-8 characters only**. The temporary password can use numbers and/or letters or a combination of both. In this case, the delegate must change their password on their next login. The new password can use numbers and/or letters or a combination of both but must be **8-30 characters**.
Will consolidated accounts display once the new strong password is created?	No. Signers will need to ensure the owner of the consolidated PAN (login ID) has changed their password to a strong password and then the signer will need to update the password on the consolidated account screen. On the Account Summary screen, the following notification will show: **Notifications** **Messages** This consolidated account cannot be viewed at this time On the Account Consolidation Manager screen: **Account Consolidation Manager** **Consolidate Account** (1/3)	Manage Delegate Access to Accounts Consolidating your accounts allows you to view all of them with a single login. You may consolidate up to 3 accounts. **Login ID** **Login ID:** ▓▓▓▓▓▓▓▓ Update PAC	Remove This consolidated account cannot be viewed at this time.

Password Reset Walkthrough

The first time that the member logs into online banking after enabling Strong Password, they will be prompted to change their password to a strong password, meeting the following requirements:

- 8-30 characters
- 1 uppercase letter
- 1 lowercase letter
- 1 number
- (Optional) may include the following special characters: @ # | $ - !

When the member logs in with their current password, they will be prompted to create a new PAC (Personal Access Code), more commonly known as their password, as shown in the screenshot below. The minimum requirements are outlined at the top of the screen.
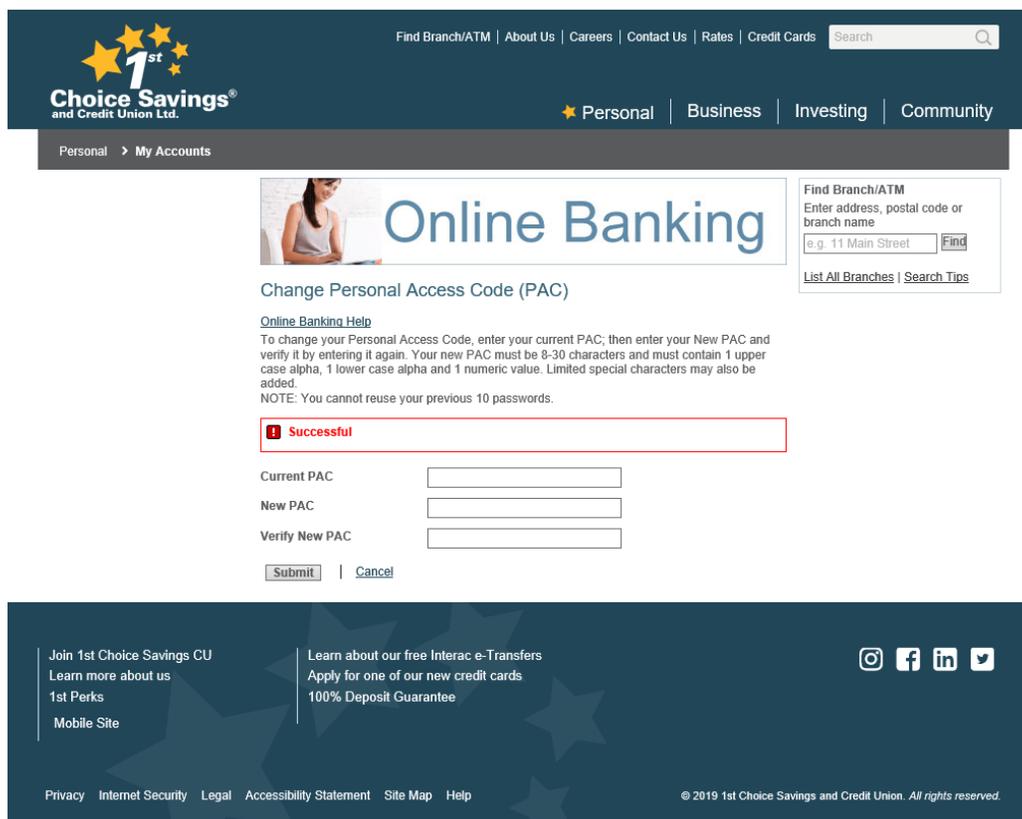
If the member's new password does not meet the minimum requirements, they will see the following error:

> ⚠️ **There appears to be an error! All errors must be corrected before continuing.**
>
> 1. The new Personal Access Code (PAC) you have entered is invalid.

Upon successful completion of the strong password reset, the member will be taken directly to the Account Summary Page in online banking.