What you need to know about
Liberty password protocols

Passwords provide your clients with the first line of defense against unauthorized access to their accounts and personal information. The stronger your client's password, the more protected his or her account will be from hackers and malicious software. To help facilitate this protection, we require strong passwords for all Liberty accounts.

Here is a reminder of the requirements currently in place for creating strong passwords and keeping your clients' information secure.

- Passwords must contain at least eight characters but no more than 32 characters.
- Passwords must contain at least three of the following:
    - Uppercase letters: A-Z
    - Lowercase letters: a-z
    - Special characters: !@#$%^&*()_+|~-=\`{}[]:";'<>?,./
    - Numbers: 0-9
    - Passwords must not contain the social or email address on the account.

For further protection, RIA passwords expire and must be re-set every 90 days. Client passwords do not expire. However, you may want to recommend to clients that they change their passwords every so often to enhance their account protection.

For even greater protection, you also have the option to turn on multi-factor authentication in Liberty. Multi-factor authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to their online account. Rather than just asking for a username and password, MFA requires one or more additional verification factors, such as answers to personal security questions, which decreases the likelihood of a successful cyber attack.

We all have a responsibility to keep our information secure. Our password protocols are designed to help keep you and your clients safe.

Please contact your Client Service Advocate if you have any questions or concerns regarding password protocols.