SHARING YOUR CONFIDENTIAL INFORMATION WITH EFP

EFP employs safeguards for the protection of personal information of our clients. These safeguard methods are employed when accessing, collecting, storing, using, transmitting, and protecting sensitive data.

These methods, some familiar, include:

A. PIN numbers to create passwords.

B. Passwords to access forms and e-sign documents.

C. Partially masking or redacting financial account and confidential personal identification numbers: Social Security, Driver's license, Passport, or state-issued identification.

D. Use Virtual Private Network (VPN) when using any public Wi-Fi.

E. Sharing and storing documents by posting electronic files to our secure (encrypted) online sites: RightCaptial Vault, Orion Client Webportal.

F. RightCapital linking /account aggregation using Yodlee's encrypted data link.

As our client, you have already begun to necessarily experience some of these safeguard measures, e.g., using PINs and passwords to access forms. In addition to those required actions, we also ask you to voluntarily follow the other methods listed above for protecting your confidential information.

Specifically, please use the methods - C, D, E - above in the following situations:

- **C - listing any financial account or personal identity numbers in any email sent to EFP.**
- **D - accessing financial accounts avoid using any public Wi-Fi or us a VPN with the public Wi-Fi.**
- **E - the information must include the whole account or personal identification numbers.**

Lastly, we cannot use/accept text messaging for any client communication because of legal compliance requirements. Please contact EFP for additional information or instructions on securely sharing and protecting your confidential information.