

PRIVACY POLICY

We are required to deliver this Privacy Policy statement to our clients annually in writing. While we would like to state categorically that clients' non-public information and data will go no further than our offices, it is more accurate to relate how such information is shared.

Our firm's four [Investment Advisor Representatives](#) store client nonpublic information on their office computers and it is archived on the firm's server, and to some extent personal information resides on the Contacts and Documents folders in the firm's online Google Apps account. All client email is archived on [Google Apps](#) servers in "the cloud." We believe our firm's server files are accessible only to Advisors, with the exception of occasional sessions by our IT maintenance person. Our firm has no other staff. Advisor computers and the firm's server are linked by our own Virtual Private Network, and we believe all channels are protected by commercially available security measures, i.e. encryption, firewall and anti-virus protection.

Support Personnel at [Fidelity Investments](#) or at any other firm that custodies and brokers client investment accounts, will have access to client personal data and to account data sufficient and necessary for them to provide their services.

We engage [BridgePortfolio, Inc.](#) (BP) to track and post client account data via a direct link to Fidelity. BP staff assimilates these data to generate monthly performance reports. Advisors can access all client account data and reports on the BP site, and clients can access only their own account data and reports with personal ID and password. BP also accesses many client accounts not custodied at Fidelity via [By All Accounts](#), which affords BP an account-owner's view of data in those accounts.

We engage [MoneyGuidePro](#) (MGP) to post client financial planning data online, accessible to the firm's four Advisors, and to clients individually by personal ID and password. Investment data in MGP is updated via a link from BP.

We use the [PreciseFP™](#) confidential online questionnaire to gather and update client personal and financial data, protected by 128-bit encryption. Clients receive a PDF version of the questionnaire, and a copy is archived on the Fountain server. PreciseFP questionnaire data maps directly onto the client's MoneyGuidePro account in the initial stage of generating a client financial plan.

Each of the entities named above strives to protect data privacy, security and integrity, motivated by internal compliance regulations, by oversight agencies, and by knowing that any breach of privacy threatens their company's survivability. On occasion we may be required by law to share client data; specifically, we will be required to open client files at random to federal and state regulators during periodic compliance audits.

Email is the most vulnerable link in the chain of data protection. Email traffic is open and accessible to the digital information world. Even though we password-protect any non-public data in email attachments, we cannot guarantee that the use of email will be completely secure.

Fountain Strategies, LLC by Douglas M. Pease, CFP®
3 July 2011 at Carmel Valley, California