The Value of Sweating the (Seemingly) Small Stuff

By Angela Carr Baker

There was a time not that long ago (or so I've heard) when bills were paid through the mail, banking required leaving your house, and most financial transactions produced a paper record for your files. When a person died, you could commonly find everything you needed to administer the estate in his or her checkbook register and filing cabinet.

For better or worse, that is not the current world we live in. The paper records of the past are now .pdf files in the cloud and file cabinets are more commonly used to store outdated mortgage documents and obsolete tax returns that should be shredded. While electronic documents, online banking and investing, and other technology tools have made many things much easier and more convenient, they have also created additional challenges when administrating estates. For example, virtual accounts that hold cryptocurrency can be extremely challenging, and sometimes impossible, to access after an account holder's death without specific detailed information that the deceased person may not have stored anywhere or told anyone about.

If you died tomorrow, how much of your financial picture could be pieced together based on the paper in your filing cabinet (or drawer, shoebox, safe, etc.), your checkbook register and your physical mailbox? In addition to the location of your estate planning and other important documents, the following is a list of the types of financial, personal and private information that you should consider having accessible to a loved one and/or a trusted advisor when you die:

FINANCIAL INFORMATION

- Life insurance policies and annuities contracts
- Other insurance policies (health, property, etc.)
- Death benefits / survivors benefits (group life, pension, deferred comp, social security, other)
- Location of bank and investment/brokerage accounts, including foreign accounts
- Location of cash, bullion, other valuables (both in or around your home or elsewhere)
- Safe deposit boxes (and notes on who has the right to access them after your death)
- Real estate holdings (list of each address or location and parcel number)
- Money owed to you (amount, debtor, location of note or other documentation of the debt)
- Business Information
    - Names of entities you have ownership in, location of documents, bank accounts, assets owned by entity, other partners, etc.
- Virtual Accounts (login info and/or access instructions)
    - Cryptocurrency Accounts
    - Mobile Payment Apps (PayPal, Venmo, Copper, etc.)
- College savings accounts or other accounts for minors (529 plans, ESAs, Washington GET credits, UTMA accounts, etc.)
- Health Savings Accounts (HSA, HRA, FSA, etc.)

- Government benefits (Veterans, SSA, etc.)

PERSONAL INFORMATION

- Location of burial instructions; funeral, eulogy, ceremony requests/instructions
- Computer, tablet, phone passwords
- Email Accounts
    - Without owner login information, access to email accounts after death depends on the provider. Some allow for limited access to content for next of kin, while many others offer no access whatsoever
- Cloud Storage Accounts (Dropbox, iCloud, Google Drive, OneDrive, Amazon etc.)
    - Similar to email, access varies by provider
- E-Reader (device itself, subscription services, access to digital library)
- Social Media Accounts (Facebook, Instagram, LinkedIn, Twitter, etc.)
    - Access to content and legacy options vary by provider. Consult terms of service/user agreements
- Membership Organizations

PRIVATE INFORMATION

Private information is anything that you want to keep private, not only during life, but also after death. This could include items that partially cross over with one of the categories above (e.g., emails, your personal photos on a computer, iPhone passcode, etc.). I recently heard a story of a man whose mother was a veracious reader and continued to be well into her nineties. After his mother died, the son was curious about her literary interests, so he looked at her Kindle Unlimited history and was shocked to find thousands of titles of erotic fiction. In that case, it is conceivable that the mother would have wanted to have a separate password for her Kindle and *not* include it with her other "important information," as otherwise recommended above.

If you find yourself particularly concerned about something being discovered after your death - whether it be your literary preferences, medications, or your stash of edibles - you may want to consider tasking a trusted friend or family member with the job of discreetly disposing of the item upon your death. If the private information is online, find out what the company's policy is for allowing access after your death. If you're satisfied with the policy, then be sure to use unique login credentials and then go ahead and take that information to the grave.

Finally, although there are numerous online tolls and products for storing passwords and other information, serious security concerns have arisen with some of them and this method of "documenting" this sensitive information should be carefully considered.

[Angela Carr Baker is an attorney, trust and estates, with Fairview Law Group PS in Seattle. Reach her at 206.753.0305 or Angela@fairviewlawgroup.com.]