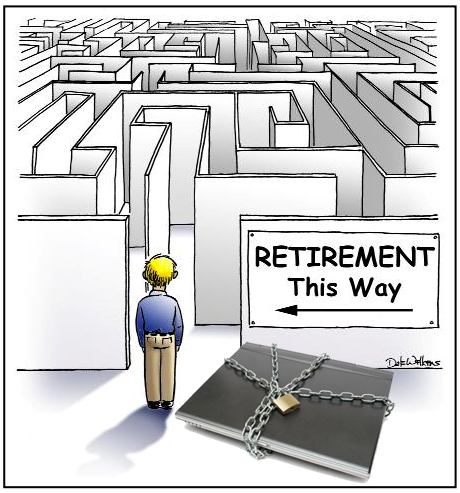
Reprinted from the
Lexington Minuteman

COROMANDEL WEALTH MANAGEMENT

January 2014

Protecting your digital legacy

Navigating the Retirement Maze



Will… Check. Durable power of attorney… Check. Health care proxy… Check. Living will… Check. IDs and passwords… Huh?

Back when I penned my first column nearly three years ago entitled *"It's Not Your Parent's Retirement,"* I described a retirement future that differed significantly from those of past generations. Part of that scenario is estate planning. In addition to all the physical and financial assets that constitute your personal estate, you have another class of assets that resides online. Thus, along with the aforementioned "Fab Four" of estate planning documents, you should now add a fifth: access to, and instructions regarding, all of your online accounts and storage locations.

We're all digital

Nowadays, our world revolves around digital communications, and our documents and records increasingly reside in what we call "the cloud." Brokerage accounts, photo repositories, purchased music, email archives… the list goes on and on.

Quick. Name all of the online accounts that you currently access. Can't do it? Well, then neither can your spouse, children, or estate executor. And face it, you probably have quite a few out there. Experian, a global credit reporting agency, found in 2012 that adults had 26 different online accounts on average; 25- to 34-year olds had 40 accounts. Thus, to make things easier for your heirs, as well as mitigate risks to your estate's financial integrity, it makes sense to document your digital assets as you would any other part of your estate.

Forecast: Legally cloudy

Unfortunately, the legal underpinnings handling for digital assets are fragmented and sometimes contradictory. Only five states have passed laws regarding the handling of digital assets, and online Web site policies – those paragraphs of arcane text we routinely ignore when clicking "I Accept" – are not standardized, and often restrict the ability to transfer the account to another person. On top of that, logging into your late father's accounts would technically violate the Federal Computer Abuse and Fraud Act. Federal privacy laws may also limit the ability of online service providers to share the accounts of the deceased with family members.

Still, the best policy for your estate's protection is to put together a comprehensive list of your digital assets, how to access them, and how you want each of them handled after you're gone. Then make sure that a few key people have access to this information.

Getting organized, digitally

The first step of a digital estate inventory is to list all of the Web sites where you have some kind of digital information stored, including credit card information, frequent flier miles, personal content, etc. If you have your own business, particularly if you are a sole proprietor, you should do this exercise separately for all of your business-related digital assets and accounts.

For each site, list the following information: Web address, site purpose, ID and password, any security Q&A (e.g., your mother's maiden name), any special verification instructions (e.g., Gmail), your personal content on the site, and instructions on what to do with the content and your account. The latter might include: Delete all information, Download all personal content and then deactivate, Maintain for six months and then delete, etc. Be explicit with your instructions, as your "digital executor" would most likely prefer not having to make this decision for every site you list.

While doing this inventory, a good security check is to look at your passwords. If any is a word that can be found in a dictionary, change it to at least 8 characters, including a number and a symbol. Otherwise, your accounts are an easy target for identity thieves, who scan obituary columns and then try to hijack the deceased's sites. A good digital asset plan will help protect against this possibility.

Tools to help

The final issue is where to store this information, which is likely to change over time. This might be a good reason to start using a password management system as a security "vault", with a single password to access all of the others. Products such as LastPass, SplashID and RoboForm2Go include optional encrypted thumb drives, making it easier to provide your access data to the limited few to whom you have given the master password.

Finally, there are a growing number of commercial Web sites for secure online document, password, and digital asset storage. These include Estate++, PasswordBox (formerly Legacy Locker), and E-Z-Safe. Prices range from free to reasonable.

Where there's a will…

… there are digital assets. Inventory and document yours, and provide a means for your heirs to access them, and you'll be eulogized as "that organized family member."

George Gagliardi is a financial advisor with Coromandel Wealth Management in Lexington, where he helps clients develop and implement investment and retirement strategies. He can be reached at (781) 728-9001 or george@CoromandelWM.com. George is affiliated with Trust Advisory Group, Ltd., a Registered Investment Advisor. This article is intended for general information purposes only, and may not be appropriate for your specific circumstances. Investment advice is particular to each individual, and should only be given after an individual situation has been reviewed.

Coromandel Wealth Management
15 Muzzey Street
Lexington, MA 02421

Phone: 781.728.9001
info@CoromandelWM.com
www.CoromandelWM.com