

GRAY & FELDMAN LLP

625 Panorama Trail Suite 1240 Rochester, NY 14625
tel. 585.218.8620 fax 585.218.8600 e-mail ggray@gfrllp.com website www.gfrllp.com

WHO CONTROLS YOUR DIGITAL LEGACY?

The internet is now used for a wide variety of activities we take for granted as part of our daily routine. We use Facebook to share thoughts and photos; Twitter and Linked-In to keep in contact; and on-line providers to manage our bank, brokerage and credit card accounts. A prudent internet user will have multiple user names and passwords to protect their accounts from being accessed by an unauthorized person. Without knowledge of the appropriate user name or password, a spouse, child or parent of a deceased or incapacitated loved one may lose control of the processes they feel is their right and obligation when memories, photos and financial information are stored on-line, encrypted, locked beyond passwords and just beyond reach.

Federal law makes access to digital assets by someone other than internet user uncertain. On the one hand, it makes it a crime for anyone to intentionally accesses "without authorization" an electronic communication; or to intentionally "exceed an authorization" to access an electronic communication. On the other hand, it also makes it a crime for an internet provider to knowingly divulge to any an unauthorized person or entity the contents of an electronic communication which it services or stores. The intricacies of the Federal law make internet providers weary of allowing anyone but the internet user access to these electronic communications and thereby impede access to loved ones of a deceased or incapacitated user.

On September 29, 2016, a bill was signed into law by Governor Cuomo which enacted New York's version of the "Uniform Fiduciary Access to Digital Assets Act" (the "Act") which nineteen (19) other states have also enacted into law. The sponsor's Memorandum in support of the Act explains its purpose this way:

[t]he wide use of digital assets has created an urgent need for legislation dealing with the administration of these assets upon the death or incapacity of the user. As a practical matter, there should be no difference between a fiduciary's ability to gain access to

information from an online bank or other Internet-based business and the fiduciary's ability to gain access to information from a business with a brick and mortar building. This measure would amend . . . [New York Law] . . . to restore control of the disposition of digital assets back to the individual and removes such power from the service provider."

The Act grants newly created access to digital assets to all types of fiduciaries; including: trustees, executors, administrators, agents under a power of attorney and guardians. They now have the authority to gain access to, manage, distribute and copy or delete digital assets. Specifically, the Act provides that a fiduciary acting within the scope of his/her/its duties is an "authorized user" for the purpose of applicable State and Federal computer-fraud and unauthorized computer-access laws.

Traditionally, service providers protect themselves by requiring a user to agree to certain terms of service ("TOS") prior to creating an online account. Some service providers have a policy that indicates what will happen upon the death of an on-line user; others did not. This created confusion and doubt as to who controlled a user's digital legacy. In a reversal of roles, a user may now, with certainty, direct the custodian of an internet account to disclose (or not to disclose) to a designated recipient some or all of the user's digital assets. This power to authorize disclosure may be exercised by the user *via* an on-line tool or in his or her will, trust, power of attorney, or other record. The direction by the user to disclose (or not disclose) digital assets overrides a contrary provision of the TOS in all cases except where the TOS require the user to act affirmatively to express direction in a manner which is distinct from the user's general assent to the TOS.

It is always prudent for a user to share with others his or her user name and password for on-line accounts. If the user did not share that information or the information is incomplete or incorrect, the Act provides a clear and certain path toward gaining access to this crucial information.

- A user may now consent in his or her Will to allow access to an Executor to the content of electronic communications sent or received by a user and stored by a custodian on the web. Accordingly, users should now draft a new Will or prepare a Codicil to their existing Will to specifically allow this access to their digital assets.

- A user may also grant access to digital assets by a power of attorney. To the extent the power of attorney expressly grants an agent the authority, a custodian must disclose to the agent the content of electronic communications sent or received by the user. The power to access electronic communications is a “hot” power and must be specifically referenced in the Power of Attorney. Accordingly, you should now execute a new power of attorney which grant the authority to access digital assets under the “Modifications” section of power of attorney.

The relief afforded by the Act should be augmented by planning for use, retrieval and disposition of digital assets. Some suggestions to aid the planning process include:

- Develop an inventory of on-line accounts and services; including how and where they are held, their user names, passwords and answers to “secret” questions. This goes contrary to the conventional wisdom of not placing the “key” to important information in one spot, so extraordinary care should be taken to insure the security of the inventory and to alert loved ones of its existence and location.

- Keep the inventory current and up to date with changes to account content or location, user names and passwords. This is perhaps the most difficult part of planning and one of the major obstacles to completing the process.

- Consider the use of an on-line “password manager” to store sensitive information. One on-line advice column (Geeksengine.com) recommends an on-line service which stores a wide range of information you may wish to keep secure. It suggests that secure information may include: e-mail account logins, credit card details, online banking login, bank account numbers, tax file number, software installation keys and website logins. It notes that a “password manager” is not just for

storing passwords. Any information that are private, sensitive, or you think should be secured can be saved to password manager. Anytime when you note down something on a piece of paper or scratch pad, or save something in a document on your computer, think if you should save the information in password manager. Password managers allow you to save your user names, passwords, and any related information and you only need to remember one master password to open the password manager program. Geeksengine.com provides one cautionary note: if you forget your master password which is used to open the password manager, all information stored in the database will be lost. Generally, there is no backdoor to the password manager that can be explored to recover your master password or other passwords stored in it.

- Consider keeping the inventory and/or master password with the original of your Power of Attorney or Will so that it is secure yet accessible.

- Consider allowing a trusted family member immediate access to these digital accounts during your lifetime so that an alternate is available to access the account if you are dead or incapacitated.

DISCLAIMER

The information contained in this brochure is provided for informational purposes only, and should not be construed as legal advice on any subject matter. No reader of its content, clients or otherwise, should act or refrain from acting on the basis of the brochure without seeking the appropriate legal advice on the particular facts and circumstances at issue. This brochure reflects a general discussion of the laws of the State of New York and of the United States only, and it may not, and probably does not, accurately reflect the law of any other State. Gray & Feldman LLP expressly disclaims all liability in respect to actions taken or not taken based on any or all the contents of this handout.

Copyright © October, 2016