Practical Planning for Passwords

By: Brian V. McAvoy and Geena G. Kandel

"Digital assets" are increasingly important in today's world. However, gaining access to these assets can be difficult in the event of incapacity or death. There are generally three categories of digital assets:

1. Personal assets.
These are typically stored on computers or other electronic devices. Examples include emails, photographs, tax returns and medical records.

2. Financial assets.
These include crypto-currency, online access to bank accounts, automatic bill paying, Amazon account or reward programs. It is important to note that while the actual funds in a bank or brokerage account are not digital assets, the on-line *access* to the account is a digital asset.

3. Social media, such as Facebook, LinkedIn or X (Twitter).
The person or institution who handles a client's affairs in the event of incapacity or death is their "fiduciary." Without proper planning, a fiduciary may have difficulty accessing these digital assets.

Here are some scenarios: (1) a fiduciary wants access to uploaded family photographs on a website or hard drive; (2) a fiduciary needs to access electronic calendar or contacts; (3) a fiduciary needs to identify electronic bills for credit cards, utilities and insurance to ensure timely payment and; (4) in the event of death, the fiduciary wants to deactivate social media accounts.

Fortunately, Facebook, Google, and Apple allow users to designate an individual to have access to their account upon the user's death. Facebook allows users to designate a "legacy contact." Upon death, the legacy contact can contact Facebook and will be granted access to the account. Apple also has an option to designate a legacy contact. Following an account holder's death, the legacy contact can make a request to Apple to gain access to certain information, including Photos, Notes, Mail, Contacts, Calendars, and Messages. Apple will verify that this person was designated as the legacy contact before providing access. Google has an "inactive account manager" which allows a user to designate a "trusted contact." Once the Google account has been deemed inactive, Google will email the trusted contact and provide the contact with the client's data in accordance with the user's instructions.

As an initial step, the client should identify all of his/her digital assets and prepare a list identifying where each digital asset is held, including usernames and passwords. This list will enable the fiduciary to locate and collect or dispose of each digital asset in accordance with the client's wishes. The list should be kept in a secure location and updated regularly. Another option is to utilize a password manager service, such as NordPass, RoboForm, Keeper, 1Password or Norton. While many password manager services are available for a fee, some companies offer a simplified free version. If a client uses a password manager, there should be a mechanism to have the master password provided to the fiduciary upon the client's death or disability.

Florida enacted the Fiduciary Access to Digital Assets Act ("FFADAA"). The FFADDA defines a "digital asset" as an electronic record in which an individual has a right or interest. The company storing digital assets is the "custodian." The FFADAA provides that if certain conditions are met, a fiduciary has the right to obtain a client's electronic communications and access their digital assets. Because the fiduciary must prove that the client consented to the disclosure, it is critical that the client's Durable Power of Attorney and Will/Trust include a provision citing the FFADDA and consenting to the custodian's disclosure of digital assets to the fiduciary.

Brian V. McAvoy, Esq. is a Florida Board Certified Attorney in Wills, Trusts & Estates and Geena G. Kandel, Esq. is an attorney with Roetzel.