Protecting Digital Assets

April 2015

Presented to the Estate Planning Council of Greater Miami

Eric Virgil, Esq.
The Virgil Law Firm
201 Alhambra Circle, Suite 705
Coral Gables, FL 33134
Telephone: (305) 448-6333
Email: eric@virgillaw.com
www.virgillaw.com

Protecting Digital Assets

I. What are Digital Assets?

"Digital assets" are electronic records that are transmitted or stored on digital devices such as smartphones and computers. Digital assets can include items such as:

(a) Documents (MS Word, Adobe PDF, Excel spreadsheets, etc.),
(b) Internet sites such as domain names or blogs;
(c) Email accounts;
(d) Social media accounts (Facebook, LinkedIn, Instagram, etc.);
(e) Intellectual property rights;
(f) Gaming characters;
(g) Online user accounts (banks, PayPal, brokerage, utilities, creditors, etc.);
(h) Business information such as customer and inventory databases, client records, and internal business accounting information (this could be part of a regular firm's record keeping or an online enterprise as found on eBay);
(i) Digital currency such as bitcoins or credits with online vendors such as iTunes; and
(j) Artistic content such as photographs.

For the purposes of this outline, it makes sense at the outset to define terms for discussion. This presentation will use definitions that were promulgated by the Digital Assets and Information Study Committee of the Real Property, Probate and Trust Law Section of The Florida Bar in their draft of a proposed Florida Fiduciary Access to Digital Assets Act. These definitions are now contained in pending Florida Senate Bill SB 102, introduced by Senator Dorothy L. Hukill. In this outline I will refer to the Florida Fiduciary Access to Digital Assets Act (SB 102) as "the Proposed Act."

Here are some definitions from the Proposed Act:

a. "Account holder" means a person that has entered into a terms-of-service agreement with a custodian or a fiduciary for such

person. The term includes a deceased individual who entered into the agreement during the individual's lifetime.

b. "Custodian" means a person/entity that carries, maintains, processes, receives, or stores a digital asset of an account holder.

c. "Digital asset" means an electronic record. The term does not include an underlying asset or liability to which an electronic record refers, unless the asset or liability is itself an electronic record.

d. "Information" means data, text, images, videos, sounds, codes, computer programs, software, databases, or the like.

e. "Terms of service agreement" ("TOS") means an agreement that controls the relationship between an account holder and a custodian.[1]

II. Where are Digital Assets Found?

Digital assets can be located on any digital device. For example, digital assets of a decedent may be located in one or more of the following places:

(a) Computers – home and office;
(b) Smartphones;
(c) Tablets;
(d) eReaders;
(e) Cameras;
(f) Memory cards and flash drives;
(g) CDs and DVDs;
(h) In the cloud (online).

[1] Terms of service agreements are those fine-print documents that pop up when establishing an online account. The computer dialog box containing the agreement typically requests that users check a box that says something like, "I have read all the terms and I agree," before the account can be created.

III. How are Digital Assets Relevant to Probate Practitioners?

Digital assets have financial value and that value can be lost. According to a 2011 survey from McAfee, Americans valued their digital assets, on average, at almost $55,000. This number is certain to be higher today. Eighty-five percent of Americans use the Internet and this is an area in which growth is rapid. The average person has 26 digital accounts and that number is higher as you deal with the younger population.

According to statistics from 2013, in just 60 seconds, there's an average of $83,000 in Amazon sales, 278,000 tweets, 72 hours of video uploaded to YouTube, 1.8 million Facebook likes, 48,000 apps are downloaded from the Apple App Store, and over 125,000 photos uploaded to various photo sharing sites. A recent study found that 75% of families with an income in excess of $75,000 conduct banking online.

To the extent digital assets have financial value, they must be marshaled, declared on inventories, accountings, and on federal estate tax returns, and administered as part of the probate process. To the extent these items are neglected or lie dormant, they may be subject to risks such as losses due to hacking, copyright violations, and termination of service from account providers. To the extent digital accounts are set to automatically pay bills, the decedent's assets may be unnecessarily lost if these autopay arrangements are not reviewed by a personal representative.

Even those digital assets without financial value likely have a sentimental value to the decedent's survivors. These assets can include photographs, emails, Facebook pages, and other personal information.

Finally, even if digital assets do not have financial value or sentimental value they contain information that point to regular assets and liabilities that fiduciaries must administer.

IV. Problems Practitioners Face With Regard to Digital Assets

The biggest problem is lack of defined right of access for fiduciaries. The Florida Probate Code, and Florida law in general, does not mention digital assets, does not define these assets, and does not contain clearly applicable rules governing access to them by fiduciaries.

More importantly, access to digital assets creates a minefield where fiduciaries can unknowingly violate both federal and state criminal law regarding hacking and privacy. Virtually none of these criminal laws have a provision for fiduciary access.

Fiduciaries also can run afoul of TOS provisions in attempting to access digital assets. One internet service provider (Google) has created a third-party access mechanism for U.S. customers, but the author is unaware of other such provider mechanisms for third parties.

As a practical matter, even if they are willing to venture into this minefield, fiduciaries may be unable to find the decedent's login and password information or information may be encrypted.

V. What Law Applies to Digital Assets?

A. Florida Law

Florida law does not specifically define or address digital assets or digital information, other than in a criminal law context.[2] To the extent Florida probate, guardianship, and trust law applies to digital assets it is now unclear how that law may be preempted or in conflict with relevant federal and Florida statutes that relate to issues such as privacy and hacking. There are no Florida cases relating to fiduciary access to digital assets or post-mortem administration of digital assets.

[2] F.S. Secs. 815.01-07 Computer-Related Crimes. For example, s. 815.06(2)(a) states – "A person commits an offense against users of computers, computer systems, computer networks, or electronic devices if he or she willfully, knowingly, and without authorization: (a) Accesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized;…." There is no explicit statutory language authorizing fiduciary access. The offense is a third-degree felony.

B. Federal Law

Federal law impacting access to digital assets relates to two areas: (1) privacy of digital information, and (2) unauthorized access to digital assets. Privacy is governed by the Stored Communications Act ("SCA") of 1986, 18 U.S.C. 2701-2711, as part of the Electronic Communications Privacy Act ("ECPA"). Unauthorized access issues are governed by the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. 1030 (1986). Both these acts date from the pre-Internet late 1980s.

The SCA, in order to protect privacy rights of individuals, prohibits providers of public communications services from disclosing the content of user's communications to third parties except in situations similar to where a warrant is obtained. Under the SCA, the originator or the addressee/intended recipient of an electronic communication may provide lawful consent for disclosure. Unfortunately, fiduciaries are not mentioned in the legislation. One issue for fiduciaries is how to provide service providers with comfort that the fiduciary can give lawful consent to disclosure of SCA protected material. Among other things, contents of emails are communications likely protected by the SCA. Further, the concept of "lawful consent" only permits disclosure by an online service provider, it does not require disclosure. This issue was litigated recently in *In re Request for Order Requiring Facebook, Inc. to Produce Documents and Things*, No. C 12 80171 LHK (N.D. Ca. Sept. 20, 2012). In that case, a decedent's family tried to compel Facebook to release account content. The court held that the SCA allowed only voluntary disclosure and that the service provider, Facebook, could not be compelled to disclose the account contents. The court did not rule on whether the personal representative possessed lawful consent of the decedent, but allowed Facebook to decide that issue.

The CFAA, on the other hand, governs access to the digital devices that would likely contain digital assets, such as computers. The CFAA requires authorization of the owner of the device in order to have lawful access. Unauthorized access is deemed to be illegal "hacking." Does a fiduciary have "authorization" of the owner to access a computer? If the fiduciary has been given express authorization, then clearly yes. If not, the law is unclear. Further, the law can be violated even with owner authorization if the fiduciary does not have the service provider's authorization. Many providers' TOS prohibit third

parties from accessing online accounts. When the fiduciary uses the account holder's authorization and login information to access an online account, does the fiduciary violate the law? Perhaps, if the access violates the TOS terms.

As a practical matter, federal and state criminal laws to prevent hacking and to preserve data privacy currently hinder disclosure and management of digital assets and information. See *Ajemian v. Yahoo*, 83 Mass.App.Ct. 565 (2013)(where there have been more than 7 years of litigation regarding the rights of the decedent's estate with regard to a Yahoo email account due to conflict regarding Yahoo's terms of service and the application of the SCA).

C. Contract Law Issues – TOS Problems

Service provider TOS frequently create legal issues related to access to digital assets. Some prohibit transfer of the assets under "indescendibility" provisions (Twitter, for example). The indescendibility concept arises from a provision in the TOS that the account/usage privileges merely constitute a license given to the account holder. Others may prohibit or inhibit fiduciary access (Instagram, Facebook, Yahoo, etc.).

D. A Proposed Solution – Florida Fiduciary Access to Digital Assets Act (SB 102)

The Proposed Act is designed to be a stand-alone act rather than legislation that addresses digital assets in piecemeal fashion in the Probate Code, the Trust Code, and so forth. The Proposed Act is divided into 9 main sections. Section 1 contains general provisions and definitions. Digital assets are defined broadly. Sections 2-5 establish the rights of personal representatives, guardians, agents acting pursuant to a power of attorney, and trustees. Sections 6-7 contain provisions relating to the rights of the fiduciary to recover property, and the rights of interested parties to object to fiduciary access. Section 8 addresses immunity from liability for compliance. The final portions of the Act address miscellaneous issues, including the effective date of the act which will hopefully be July 1, 2015.

The Proposed Act is a solution to the bigger roadblocks to fiduciary access. The Proposed Act does the following:

(a) Define digital assets and related terms;

(b) Provide clear default rules for fiduciary access. The fiduciary has the same right of access as the account holder/owner except where the account holder/owner explicitly opts out of fiduciary access (this eliminates most TOS issues);
(c) Allow for account holder/owner intent and privacy desires as the account holder/owner's stated intent would govern. The default rule would allow for fiduciary access, as is currently the custom in probate for non-digital assets but the owner can state otherwise;
(d) Encourages provider/custodian compliance and establishes clear procedures for provider/custodian interaction with fiduciaries;
(e) Provides protection from liability for fiduciaries and providers/custodians; and
(f) Clarifies that the Proposed Act is inapplicable to digital assets of employers used by employees in the ordinary course of the employer's business.

The Proposed Act makes only governs access to digital assets. The underlying ownership and title of assets is not changed by the Proposed Act. Asset title and ownership would be governed by existing law.

The Proposed Act was carefully written to fit into the framework of the SCA and the CFAA so as not to be preempted by those laws but rather to fit into their scope in a defined way so that authorized access is clarified for all interested parties.

VI. What Can be Done to Plan for and Protect Digital Assets?

A. Estate Planning - Advise Clients to Plan Ahead and Provide Tools

While estate planners, fiduciaries, and fiduciary counsel have perfected techniques used to transfer long-established types of property, most attorneys and fiduciaries have not yet determined how to address the disposition of digital assets. In addition, few owners of digital assets consider the fate of their online accounts or information once they are no longer able to manage these assets.

During the estate planning process, clients can be advised to plan ahead. Such planning includes advice to clients to do the following: (1) conduct a digital inventory; (2) back up (especially locally and to tangible media devices such as

USB hard drives, flash drives, DVDs, etc.) their electronic information; and (3) make an estate plan that includes digital asset provisions. A tool for conducting a digital inventory is the My Digital Audit form attached to this outline as Exhibit A.[3]

The client should be informed they may supplement a paper record, such as My Digital Audit, with additional online measures. Online measures include: (1) use of an electronic service that safeguards passwords and logins, such as 1Password or LastPass; and (2) post-mortem online planning through companies like DeathSwitch, LegacyLocker, SecureSafe, that allow you to designate and approve access by fiduciaries prior to their appointment.

In all of this planning, there is a security risk tradeoff the client must weigh in terms of giving vendors (or a third party such as the attorney) password information versus keeping passwords to themselves in a secure place such as a safe deposit box or some other secure location. There is significant hassle cost with regard to this recordkeeping since password and login information changes regularly. I would not advise the attorney to keep this information for the client due to the security issues involved.

With regard to backed-up information, to the extent it is local this is helpful as it allows fiduciaries to avoid the current potential legal problems associated with accessing data stored remotely with service providers.

The client's estate planning documents should be drafted to include language aimed at administration of digital assets and information. Digital assets should be defined in the document if specifically devised. Fiduciary powers over digital assets should be set forth in the documents. One area that is evolving here is the possible use of trusts for digital assets that are otherwise "indescendible" (such as license-based assets that expire on death). Wills, of course, should not contain passwords or any login information since wills become public records.

---

[3] The author thanks James D. Lamm, Esq. of Minneapolis, MN, who graciously shared this form and shared additional information with the author in the preparation of this presentation. Mr. Lamm's blog, www.digitalpassing.com, is a great digital estate planning resource.

Sample forms[4] relating to fiduciary powers are set forth in Exhibits B (for powers of attorney), C (for wills), and D (for trusts). ***Please use caution with regard to any review of these forms, as noted in the beginning of the outline. The forms are drafted broadly so to the extent a client desires to limit access that limitation needs to be drafted into the planning.***

As noted above, one problem with planning ahead and doing digital audits is that logins and passwords frequently change; computers crash or wear out and are replaced. There is certainly a hassle-cost to this kind of planning but some planning is better than no planning.

One final tip relates to the email account-centric nature of digital assets. Most digital assets are linked to a particular email account of the account holder/owner. Therefore, one (not several) personal (not work) email account should be linked to a person's digital assets. If a work email account is used, the fiduciary may not be able to access that account since an employer can lawfully deny access to the account.

VII. How to Handle Probate of Digital Assets As the Law Evolves?

A. Select Appropriate Personal Representatives and Empower Them

The designated personal representative does not need to be a technical genius but should be able to work with or find people knowledgeable about computers and technology. If the personal representative is uncomfortable or unable to handle technical matters, consider recommending the retention of a computing expert to consult with the personal representative. The consultant can review digital issues, make recommendations for action to the personal representative, and leave the personal representative free to handle more traditional administration matters.

With regard to digital assets the personal representative should be granted the broad powers, including the power to hire consultants to assist the personal

[4] The materials in this outline, and the attached exhibits and forms, are intended for continuing legal educational purposes only. They are not to be construed or relied upon as legal advice. The forms are sample forms only and should be used or adopted, if at all, only after careful independent consideration and review.

representative with appropriate actions. See Exhibit C for a sample powers clause for a will.

B. Steps the Personal Representative Can Take

Digital assets present new challenges for fiduciaries. Fiduciaries have duties with regard to these assets but no clear rights regarding access. With regard to determining assets and creditors, previously fiduciaries could rely on searches of paper records in homes, offices, and of items sent in the mail. Mail is now almost a thing of the past and people receive their notices, pay bills, conduct banking, and receive financial statements online. The personal representative also will be challenged in determining how to value digital assets. Finally, the personal representative will have to overcome electronic tripwires such as passwords and encryption.

Unless and until the Proposed Act passes, the personal representative should seek a specific court order giving the personal representative detailed authority to access digital assets and to hire consultants as necessary to assist in that regard.

The personal representative must determine which digital devices exist and their ownership. The devices used by the decedent and found by the personal representative (such as tablets or smartphones) may be owned by an employer or another person, so care needs to be taken to confirm ownership and the extent of the personal representative's authority over any devices.

Before the personal representative attempts to use the devices or power them on, the personal representative should consider retaining a computer consultant or forensics company to be the first to handle the devices. The consultant can be directed to make exact copies of what is contained on the devices prior to any other action taking place. If the personal representative wants to attempt this individually, there is software available to assist with this task.

The retention of a computer expert can save the personal representative much time in determining what issues exist. Once the personal representative has access to the digital information of the decedent then the personal representative must determine what digital assets exist.

C. Determining What Digital Assets Exist in the Estate and Administering These Assets

Information located on smartphones, computers and email, and voicemail help you find digital assets located in online accounts/in the cloud. You should physically secure devices as they contain digital information but are also tangible personal property of the decedent (or of others).

Look for information about digital assets by searching the decedent's computer favorites folders and favorites websites, bookmarked websites, browsing history, and emails from accounts and service providers. Look for financial software or digital wallet software (for digital currency such as bitcoins) on devices. Video game characters and items, such as game property and points, can have financial value. Review income tax returns. Order a credit report for the decedent. Finally, the decedent may have data stored online (in the cloud). A combination of paper review and digital review will be required to determine the decedent's assets.

Regular email accounts will normally grant a personal representative access to contents but not full use of account (this varies). The personal representative or counsel should review the TOS for the accounts, email and otherwise. Most providers will allow access by next of kin; will usually require proof of relationship and proof of death before access allowed. In most cases, ownership of the account is not transferred to the fiduciary or family member. Terms for e-mail providers can be restrictive (such as Yahoo) or more relaxed (such as Gmail). An email account may be deleted or terminated if not accessed or updated within 4 to 6 months. Email accounts should not be closed prior to ensuring that the decedent's financial information sent periodically by email (such as account statements and bills) and a record of the contents of the account have been saved. Email addresses should be changed with regard to delivery of financial information and bills.

With regard to the decedent's devices, the personal representative should be advised to get the data from the devices and back that data up. Get help from a computer expert for how to get information off devices and access it in the first place if family members can't provide access and you don't have password information of the decedent.

Under current law, filing lawsuits to get information and gain control over digital assets is a strategy with significant drawbacks. Lawsuits are slow and expensive and you likely will run into legal problems such as the SCA issues raised in the *Ajemian* case. In addition, litigation to gain access to employer email accounts is unlikely to be successful for a variety of reasons.

Unless the Proposed Act passes, the personal representative should only use the decedent's passwords on a very temporary basis (if at all) until they can be legally changed for the personal representative's use. As discussed above, use of the decedent's passwords may be deemed legally unauthorized.

The personal representative should consider wiping out the memory of the devices, using forensic deletion standards and software, prior to transferring them to the ultimate beneficiary. However, if the device is an e-reader or music device (like an iPod) the personal representative may want to consult with the beneficiary with regard to keeping books or music on the device.

If you can determine which financial institutions the decedent used, you can request paper copies of statements and information.

Determine whether the decedent had accounts with online sales organizations such as eBay, Amazon, or Craigslist (look for PayPal or Western Union information in records). Online purchasing accounts can be found through credit card receipts and bank receipts. Look for iTunes or Amazon cards. Credit card receipts can also show rewards programs, such as AMEX Member Rewards. For each rewards program discovered, the personal representative should contact the administrator of the program (i.e., AMEX) and follow their procedures in order to transfer the rewards points to the appropriate beneficiaries. A copy of the AMEX policy for transfer of rewards points is attached as Exhibit F.

Unfortunately, access to information and rewards points can be lost if accounts such as email accounts or credit card accounts are closed. As noted above, the personal representative should not close the decedent's accounts until full information regarding the account and any potential benefits in the account have been marshaled.

Webpage, domain name ownership, and blog information can be found through emails and credit card statements which set forth charges from providers or show reminders in emails to renew the domain. Domain ownership can be searched using WHOIS services and online services such as domaintools.com. Ownership of domains can be transferred to beneficiaries but new owner needs to confirm transfer.

Social networks should be contacted regarding death of the decedent. Their policies vary regarding what can be done post-death with the accounts.

To the extent digital accounts are set to autopay bills, the decedent's assets may be unnecessarily lost if autopay arrangements are not reviewed by a personal representative. However, make sure that online accounts are maintained until the personal representative can determine the value associated with those accounts and retrieve relevant information from the accounts.

D. How to Value Digital Assets?

Smartphones and computers have some value as tangible personal property. However, they need to be marshaled and examined mainly due to the data they contain. The value of the data itself is discussed further below.

Email accounts likely have little financial value unless the person was a celebrity. For online purchase and sales accounts (PayPal, Amazon, iTunes) review emails and statements to find them and then contact the institution to get cash balances as necessary. Online sales accounts may have value as ongoing business (may need business valuation).

Web pages and blogs normally have no financial value unless the decedent had a wide online audience. Social networking is similar to web pages and blogs in terms of financial valuation.

Domain names normally don't have value but may if popular terms are involved. Beer.com sold for $7 Million Dollars, vodka.com sold for $3 Million Dollars. Domain name appraisal services do exist (for example, Afternic).

Digital intellectual property rights may have value and, if so, are valued according to their past and future revenue streams.

With regard to games there is a market for gaming characters, items and currency depending upon the game and the decedent's level of achievement.

Digital currency has a monetary value which can be determined online depending upon the type of currency involved.

For federal transfer tax purposes, IRC Sec. 2031 and Reg. 20-2031-1(b) apply like they would to traditional property. This means you look for comparable sales, cash flows, auction value, etc. Since this is a new area this is easier said than done. Comparable sales are hard to find and historical costs are hard to determine in this area. This is an area where use of an expert to appraise the property will be helpful.

These assets may have different classifications. For example, computers and smartphones are tangible personal property. Domain names are intangible property. The personal representative will need to classify property appropriately.

E. Finally, What About Music, Photos, and Apps?

Smartphones, e-readers, and other devices such as iPods will contain digital media such as music, books, photos, and apps. Look for iTunes and Amazon accounts of the decedent. Many times an account will have a cash balance that can be liquidated. With regard to photos online, review whether the decedent had accounts with photo sharing websites such as Flickr.

Can a personal representative sell or transfer digital media files without violating copyright laws? At this point you are likely asking for trouble if you sell or transfer files separately from device itself so that is not recommended. See *Capital Records v. ReDigi*, 2013 WL 1286134 (S.D.N.Y. 2013).

Exhibit A

See attached My Digital Audit Form
(Courtesy of James D. Lamm, Esq.)

My Digital Audit:
Passwords, Online Accounts, & Digital Property

Voicemail & Home Security Systems

Name: _____

Home address: _____

Telephone #: _____

Voicemail # & password: _____ _____

Security company & phone #: _____ _____

Security system password: _____

Vacation home address: _____

Telephone #: _____

Voicemail # & password: _____ _____

Security company & phone #: _____ _____

Security system password: _____

Business address: _____

Telephone #: _____

Voicemail # & password: _____ _____

Personal cell phone # & password: _____ _____

Voicemail # & password: _____ _____

Business cell phone # & password: _____ _____

Voicemail # & password: _____ _____

Safe/lockbox location & combination: _____ _____

Safe/lockbox location & combination: _____ _____

Other: _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

Computer Passwords

Home computer #1 description: _____

Username & password: _____ _____

Username & password: _____ _____

Username & password: _____ _____

Username & password: _____ _____

Home computer #2 description: _____

Username & password: _____ _____

Username & password: _____ _____

Username & password: _____ _____

Username & password: _____ _____

Home computer #3 description: _____

Username & password: _____ _____

Username & password: _____ _____

Username & password: _____ _____

Username & password: _____ _____

Office computer #1 description: _____

Username & password: _____ _____

Office computer #2 description: _____

Username & password: _____ _____

Other devices: _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

E-Mail Accounts

E-Mail Provider	E-Mail Address	Password
Home e-mail:		
Work e-mail:		
Microsoft Outlook/Hotmail:		
Yahoo! Mail:		
Google Gmail:		
Other:		

Social Networking Accounts

Service	Username	Password
Facebook:		
LinkedIn:		
Google+		
MySpace:		
Twitter:		
Foursquare:		
Other:		

Instant Messaging, Chat, & Videoconference Accounts

Service	Username	Password
Skype:		
AOL Instant Messenger:		
Yahoo! Messenger:		
ICQ:		
Google Talk:		
Jabber:		
Other:		

Financial Accounts

Intuit Quicken software password: _____

Mint.com username & password: _____ _____

PersonalCapital.com username & password: _____ _____

PowerWallet.com username & password: _____ _____

Tax preparation software password: _____

Bank #1 name & Web address: _____ _____

Username & password: _____ _____

ATM/debit card PIN: _____

ATM/debit card PIN: _____

Bank #2 name & Web address: _____ _____

Username & password: _____ _____

ATM/debit card PIN: _____

ATM/debit card PIN: _____

Brokerage #1 name & Web address: _____ _____

Username & password: _____ _____

ATM/debit card PIN: _____

ATM/debit card PIN: _____

Brokerage #2 name & Web address: _____ _____

Username & password: _____ _____

ATM/debit card PIN: _____

ATM/debit card PIN: _____

Credit card #1 name & Web address: _____ _____

Username & password: _____ _____

PIN: _____

Credit card #2 name & Web address: _____ _____

Username & password: _____ _____

PIN: _____

Financial Accounts (Continued)

Credit card #3 name & Web address: _____ _____

Username & password: _____ _____

PIN: _____

Credit card #4 name & Web address: _____ _____

Username & password: _____ _____

PIN: _____

Credit card #5 name & Web address: _____ _____

Username & password: _____ _____

PIN: _____

Other: _____ _____

Domain Names, Web Pages, & Blogs

Domain Name & Registrar/Host	**Username**	**Password**

Online Storage Accounts

Website	**Username**	**Password**
Apple iCloud:		
Dropbox:		
Google Drive:		
Microsoft OneDrive:		
Other:		

Online Shopping & Auction Accounts

Website	**Username**	**Password**
Amazon:		
Barnes & Noble:		
Craigslist:		
Ebay:		
PayPal:		
Western Union:		
Other:		

Video Games & Virtual Worlds

Website	**Username**	**Password**

Intellectual Property

Website or Other Location	**Username**	**Password**
Instagram:		
Flickr:		
Photobucket:		
SmugMug:		
YouTube:		
Vimeo:		

Digital Music, eBook, Video and Other Media Accounts

Website	**Username**	**Password**
Amazon Kindle/Prime:		
Apple iTunes:		
Barnes & Noble Nook:		
Hulu:		
Netflix:		
YouTube:		
Other:		

Other Online Accounts

Website	**Username**	**Password**

Other Online Accounts

Website	**Username**	**Password**

Exhibit B

Sample language for a durable power of attorney*:

I authorize my Agent to access any digital assets I own or in which I am an account holder, either in my own name or jointly with anyone, including but not limited to online accounts relating to email, banks, brokerage firms, Internet service providers, retail vendors, utilities, mutual funds and the like; to open new accounts and close accounts as my Agent determines is necessary or advisable and in my best interests; and to transfer funds among my online accounts as my Agent deems necessary or advisable. In order to exercise the authority granted above, I further authorize my Agent:

- **(a) To access, use, and take possession and control of my digital devices including, but not limited to, desktops, laptops, tablets, peripherals, storage devices, mobile telephones, smartphones, and any similar digital device; and**
- **(b) To take such actions as necessary, including employing agents to assist my Agent in decrypting any encrypted electronically stored information of mine or to recover or reset any password or other kind of account "sign in," login, username, or authorization in order to access any digital device or digital asset of mine.**

I authorize any person or entity that possesses, has custody, or controls any digital assets of mine, including but not limited to online accounts or electronically stored information of mine, to divulge to my Agent any electronically stored information of mine; the contents of any communication that is in electronic storage; and any records pertaining to me maintained by that person or entity. This authorization is to be construed as my lawful consent under the Electronic Communications Privacy Act (including the Stored Communications Act thereunder); the Computer Fraud and Abuse Act; and any other applicable federal or state data privacy law or criminal law.

***This grant of power is very broad. To the extent the principal desires to limit the Agent's authority, those limitations would need to be added to the power of attorney document.**

Exhibit C

Sample language for a will*:

I grant to my Personal Representative full power and authorization to deal freely with any digital assets in my estate. The Personal Representative may exercise all power and authority over my digital assets that an owner and/or account holder of the digital asset would have. "Digital assets" mean electronic records such as electronically stored information of mine, online accounts, domain names, etc. In order to exercise the authority granted above, I further authorize the Personal Representative:

(a) To access, use, and take possession and control of my digital devices including, but not limited to, desktops, laptops, tablets, peripherals, storage devices, mobile telephones, smartphones, and any similar digital device;
(b) To take such actions as necessary, including employing agents to assist the Personal Representative, in decrypting any encrypted electronically stored information of mine or to recover or reset any password or other kind of account "sign in," login, username, or authorization in order to access any digital device or digital asset of mine; and
(c) To securely delete the following digital assets: _____ _____.

I authorize any person or entity that possesses, has custody, or controls any digital assets of mine, including but not limited to online accounts or electronically stored information of mine, to divulge to my Personal Representative any electronically stored information of mine; the contents of any communication that is in electronic storage; and any records pertaining to me maintained by that person or entity. This authorization is to be construed as my lawful consent under the Electronic Communications Privacy Act (including the Stored Communications Act thereunder); the Computer Fraud and Abuse Act; and any other applicable federal or state data privacy law or criminal law.

***This grant of power is very broad. To the extent the testator desires to limit the Personal Representative's authority, those limitations would need to be added to this language.**

Exhibit D

Sample language for a trust*:

I grant to my Trustee full power and authorization to deal freely with any digital assets in my trust estate. The Trustee may exercise all power and authority over my digital assets that an owner and/or account holder of the digital asset would have. "Digital assets" mean electronic records such as electronically stored information of mine, online accounts, domain names, etc. In order to exercise the authority granted above, I further authorize the Trustee:

(a) **To access, use, and take possession and control of my digital devices including, but not limited to, desktops, laptops, tablets, peripherals, storage devices, mobile telephones, smartphones, and any similar digital device, if the digital device has been transferred into the trust;**
(b) **To take such actions as necessary, including employing agents to assist the Trustee, in decrypting any encrypted electronically stored information of mine or to recover or reset any password or other kind of account "sign in," login, username, or authorization in order to access any digital device or digital asset of mine;**
(c) **Upon my death to securely delete the following digital assets:**
_____
_____.

I authorize any person or entity that possesses, has custody, or controls any digital assets of mine, including but not limited to online accounts or electronically stored information of mine, to divulge to my Trustee any electronically stored information of mine; the contents of any communication that is in electronic storage; and any records pertaining to me maintained by that person or entity. This authorization is to be construed as my lawful consent under the Electronic Communications Privacy Act (including the Stored Communications Act thereunder); the Computer Fraud and Abuse Act; and any other applicable federal or state data privacy law or criminal law.

***This grant of power is very broad. To the extent the settlor desires to limit the Trustee's authority, those limitations would need to be added to this language.**