Planning for an Electronic Age: What are Digital Assets? How are they Identified? Valued? Distributed? How do Fiduciaries Gain Access?

National Capital Gift Planning Council
January 14, 2015

Anne W. Coventry, Principal
Pasternak & Fidis, P.C.
Bethesda, Maryland
acoventry@pasternakfidis.com

Karin Prangley, Midwest Regional Trust Head & Wealth Planner
Brown Brothers Harriman & Co.
Chicago, Illinois
karin.prangley@bbh.com

I. Advances in technology have changed both planning and administration for estates and trusts

A. Valuable digital assets should be addressed in the estate planning and administration processes. For almost all clients, and increasingly, an estate plan that does not address digital assets is not adequate. Unfortunately, not everyone will plan for digital assets, and many fiduciaries will find themselves in a difficult position, without access to (and sometimes without knowledge of) digital assets.

B. Because digital assets can be valuable, if a fiduciary overlooks the digital assets of the decedent/grantor/principal/ward, the fiduciary may be liable for waste and may leave the principal vulnerable to identity theft and the loss of valuable data.

II. Definition of digital assets

A. "Text, images, multimedia information, or personal property stored in a digital format, whether stored on a server, computer or other electronic device which currently exists or may exist as technology develops, and regardless of the ownership of the physical device upon which the digital asset is stored. Digital assets include, without limitation, any words, characters, codes or contractual rights necessary to access the digital assets." Oregon State Bar Legislative Proposal to amend, among other provisions, OR. REV. STAT. 111.005 (2013).

B. "'Digital asset' means a record that is electronic. The term does not include an underlying asset or liability unless the asset or liability is itself a record that is electronic." Fiduciary Access to Digital Assets Act, § 2(9) (July 2014) (copy available at http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets).

C. Includes:

1. Email Accounts

2. Email messages and other electronic communications protected under federal privacy laws

3. Smartphones, tablets, netbooks and computers

4. Online Sales Accounts (e.g., eBay, Amazon, Etsy)

5. Online Purchasing Accounts (e.g., PayPal)

6. Online Storage Accounts / Cloud Storage Accounts (e.g., DropBox, Shutterfly, Google Drive)

7. Webpages

8. Domain Names

9. Blogs

10. Social Networking Accounts (e.g., Facebook, Twitter, LinkedIn)

11. Intellectual Property Rights in Digital Assets

III. Why are digital assets relevant to estate planning or administration

A. A digital asset can be the key to unlocking other assets ("hard assets") with financial value.

1. Example: a decedent's email account that contains bank and brokerage statements. The bank or brokerage assets are hard assets and if the fiduciary can locate them she can access them via traditional means.

2. But technology has complicated the process even for these hard assets, because if the decedent received electronic statements and has no other evidence of the existence of the account, the fiduciary may not discover the financial account itself without access to the email account.

B. Digital assets themselves can also have financial value.

1. Domain names can have tremendous value.

(a) MI.com sold for $3.6 million in April of 2014 (top 2014 sale)

(b) Vacationrentals.com sold for $35 million in 2007

2. Blogging can generate revenue and in many cases, a blog should be treated as a valuable business.

(a) In November 2011, The Atlantic reported that America's top 10 most valuable blogs have an estimated aggregate value of $785 million.

(b) The #1 most valuable blog in 2011 was gawker.com – valued at $318 million (more than the next 5 combined) with $53.6 million in ad revenue in 2010.

3. Even a username may have value. Naoki Hiroshima, owner of the one-letter Twitter handle @N, was offered as much as $50,000 for it (although the sale of the Twitter handle would have been a violation of Twitter's terms of service). Many failed attempts had been made to steal the Twitter handle before a hacker successfully broke into Hiroshima's GoDaddy email account, PayPal account and Facebook account and changed all of the registration information to keep the legitimate account holder out. The hacker then used this as leverage to extort the precious Twitter handle from Hiroshima. Naoki Hiroshima posted a detailed account of how the theft occurred and, after a month of investigating, Twitter eventually restored @N to him.

4. Online businesses certainly have value. Former attorney and eBay seller Linda Lightman, owner of the eBay designer consignment shop "Linda's Stuff," has gross sales of approximately $20 million per year.

C. Digital assets may carry non-financial value or indirectly implicate financial value.

1. Preserving the decedent's story and memories: historically, shoeboxes of the decedent's letters, photos and diaries were treasured. The new "digital shoebox" includes:

(a) Online photo accounts

(b) Personal blogs

(c) Email messages

(d) Twitter feeds

2. Preserving a decedent's work/hobby efforts: Genealogical information is commonly stored online on websites such as Ancestry.com; the decedent may have created digital artwork.

3. Preventing disclosure of secrets and reputation preservation: protecting the sensitive information of the deceased/disabled person is often important to prevent family members from emotional suffering. With full access to the client's digital assets it is easier to preserve and protect sensitive or confidential information.

4. Minimizing risk of identity theft: The AARP estimates that the identities of 2.5 million deceased Americans are subject to fraud each year and concludes that the crime often begins with a search of online information. Careful censure of online information about the decedent (such as dates of birth, names of family members – specifically mother's maiden name – and place of residence) is critical to preventing fraudulent activities.

5. Protecting the fiduciary: if a decedent set up automatic payments from his accounts for various recurring expenses, gaining early access is essential for the fiduciary to shut off automatic payments. In an insolvent estate, failure to shut them off could mean paying creditors out of order. For any estate, payments that simply should not be made (e.g., renewal of subscriptions or memberships for the decedent) should be stopped to avoid waste.

IV. Obstacles to fiduciary access

A. Proper planning for digital assets is complicated by certain obstacles to access: knowing the digital asset exists (lack of a paper trail makes it difficult); having the means to access the asset (username and password); and getting proper authorization to access the asset. Proper authorization goes beyond merely having the username and password, or even having the express written authorization of the account holder. This obstacle is not only serious, it is also

counterintuitive to many estate planners accustomed to the plenary authority of legally appointed fiduciaries: there is potential criminal liability for access by a legally appointed fiduciary.

B. The terms of service of many digital asset providers state that only the user – and not his legal successors (e.g., duly appointed personal representative, trustee or agent under a power of attorney) – is authorized to access the user's account, regardless of whether the user is deceased or disabled, and regardless of whether the user expressly consented to his fiduciary's access. For example, Yahoo!'s terms of service provide:

> No Right of Survivorship and Non-Transferability. You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted.

C. Federal and state laws criminalize certain types of unauthorized access or damage to computers or data. What does "unauthorized" mean? A surviving spouse may assume that if her husband gave her his username and password with the intent that she would be able to access the data after his death, she has been authorized to access the data, but she would be mistaken. If the digital asset provider's terms of service do not authorize the fiduciary to access the deceased or disabled user's account, then access by the fiduciary is a violation of these criminal laws. Only the service provider's terms of service can "authorize" the fiduciary's access.

D. All fifty states have criminal laws prohibiting unauthorized access to electronic data. A helpful chart of such laws can be found at: http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx

E. Maryland has made it a misdemeanor punishable by up to 3 years imprisonment or a fine of up to $1,000, or both, to intentionally, willfully, and without authorization: (i) access, attempt to access, cause to be accessed, or exceed the person's authorized access to electronic data; or (ii) copy, attempt to copy, possess, or attempt to possess electronic data so accessed. MD. CODE ANN., Crim. Law § 7-302 (2013).

F. The Computer Fraud and Abuse Act ("CFAA"), enacted in 1986, makes it a federal crime to intentionally access a computer without authorization or exceeding authorization and thereby obtain financial data or information from a computer system. 18 U.S.C. §1030 (2013).

1. The U.S. Department of Justice has stated that violating a term of service on Facebook or Match.com is a federal crime under the CFAA; however, it is not the Department's intention to prosecute "minor" violations. U.S. v. Nosal, 642 F.3d 781(9th Cir. 2011); see also, Cyber Security: Protecting America's New Frontier, Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec., House Comm. on the Judiciary, 112th Cong. (2011) (statement of Richard Downing, Deputy Chief, Computer Crime and Intellectual Prop. Sec., Crim. Div., Dep't of Justice).

2. The DOJ prosecuted a mother under the CFAA who violated MySpace's terms of service by lying about her identifying information, including age (she posed as a 17-year-old and cyber-bullied her daughter's classmate). U.S. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

3. Many courts have interpreted the CFAA narrowly, holding that the crime of exceeding authorized access occurs only where there has been a violation of restrictions on access to information, and not where there has been a violation of restrictions on its use (i.e., misappropriation). See, e.g., Nosal, id.; LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962 (D. Ariz. 2008); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373 (S.D.N.Y. 2010); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322 (N.D. Ga. 2007); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479 (D. Md. 2005).

G. The Stored Wire and Electronic Communications and Transactional Records Access Act, enacted in 1986 ("SWA") prohibits digital asset providers that provide electronic communication services to the public from voluntarily disclosing the contents of electronic communications to anyone unless an exception applies. There is no exception for fiduciary access upon death or disability. There is, however, an exception if the user provides lawful consent to the disclosure, in which case the provider may (but is not compelled to) disclose the contents of the electronic communication. 18 U.S.C. Chapter 121 (2013).

1. An unanswered question is whether the personal representative, standing in the shoes of the deceased or disabled user, could provide lawful consent to disclosure under the SWA. If lawful consent is conveyed, providers are not compelled to disclose the contents of the electronic communication, but they may do so at their discretion without liability under the SWA.

2. The Uniform Fiduciary Access to Digital Assets Act, which is described in detail in Article V.B below, provides that a fiduciary has the lawful consent of the account holder to disclosure of protected electronic communications.

3. In 2012, a federal judge in California granted Facebook's motion to quash a subpoena from representatives of former beauty queen Sahar Daftary's estate to gain access to her Facebook account. In re Request for Order Requiring Facebook, Inc. to Produce Documents and Things, C 12-80171 LHK (PSG) (N.D. Cal.; Sept. 20, 2012). Sahar's personal representative brought a civil action against Facebook to release the contents of her Facebook account in an effort to prove her state of mind at the time of her alleged suicide. The ruling stated that civil subpoenas do not compel disclosure under the SWA, and Facebook was within its rights to deny the request for disclosure. The court stated that "nothing prevents Facebook from concluding on its own that Applicants have standing to consent on Sahar's behalf and providing the requested materials voluntarily." This provides hope that perhaps a personal representative can grant lawful consent to disclosure under the SWA.

H. Under these evolving standards, a fiduciary does not have authorized access (no matter the use or purpose and no matter if the account owner gave him or her the password) if

the terms of service of the applicable digital asset provider prohibit it. If the fiduciary accesses the user's account without authorization (i.e., in violation of the terms of service), the fiduciary is in violation of the CFAA. The SWA ensures that online service providers are not likely to extend access to fiduciaries under their terms of service. A surviving spouse may be willing to take the risk, but would a professional fiduciary? And would the attorney for a fiduciary be willing to counsel his or her client to do it? Don't count on it.

V. Aids to fiduciary access

A. Increasingly, state legislatures are providing express statutory authority to allow fiduciaries to access and control certain digital assets of a deceased or disabled person. Eight states currently have such legislation.

1. Delaware has adopted a version of the Uniform Fiduciary Access to Digital Assets Act (discussed below). DEL. CODE TIT. 12 §5001 et seq. (2014)

2. Connecticut gives a personal representative the power to access or copy the contents of the decedent's email account. CONN. GEN. STAT. § 45a-334a (2014).

3. Idaho gives a personal representative and a conservator the power to "take control of, conduct, continue or terminate" a decedent's or principal's email account, social networking profile, blog or short message service account. IDAHO CODE §§ 15-3-715(28) and 15-5-424(3)(z) (Michie 2013).

4. Indiana allows a personal representative to access or copy any of the decedent's electronic documents or information. IND. CODE § 29-1-13-1.1 (2013).

5. Nevada gives a personal representative the power to terminate an online account or digital asset. NEV. REV. STAT. § 143.188 (2011).

6. Oklahoma's statute is substantially identical to the Idaho statute. OKLA. STAT. 58 § 269 (2013).

7. Rhode Island General Laws Chapter 33-27 is substantively identical to the Connecticut Statute. R.I. GEN. LAWS §§ 33-27-1–33-27-5 (2013).

8. Virginia gives a personal representative of a deceased minor's estate some rights to consent to the release of the minor's communications under the SWA. VA. CODE ANN. § 64.2-110 (Michie 2013).

9. Maryland has not yet adopted any law granting fiduciary access to digital assets. A bill was introduced during the 2013 Regular Session that would have allowed a personal representative to take control of, conduct, continue, or terminate an account of a decedent on a social networking website, microblogging or short messaging service website or electronic mail service website. S.B. 29, 2013 Gen. Assemb., Reg Session. (Md. 2013).

However, the bill was defeated after discussions with the sponsor, in order to await the model act from the Uniform Law Commission (see below).

10. At present, none of these laws expressly supersede conflicting provisions in the terms, conditions and privacy policies of online providers. Fear of potential penalty under the CFAA for unauthorized fiduciary access remains.

B. Uniform Fiduciary Access to Digital Assets Act

1. In January of 2012, the Uniform Law Commission ("ULC") approved a study committee on a fiduciary's power and authority concerning digital assets of a disabled or deceased person. The study committee formed a drafting committee to create a free-standing act (rather than patchwork amendments to ULC acts, such as the Uniform Probate Code, the Uniform Trust Code, the Uniform Guardianship and Protective Proceedings Act, and the Uniform Power of Attorney Act) that will vest personal representatives, trustees, guardians/conservators, and agents under a power of attorney with the authority to access digital assets.

2. The ULC approved the Committee's final draft in July 2014 and in October of 2014, it became available to the public in final form for adoption in interested states. Delaware has already adopted a version of it, and the Section Council of the MSBA's Estates & Trust Law Section is working on a draft bill to put forward for enactment in Maryland.

3. The Uniform Fiduciary Access to Digital Assets Act ("UFADAA") provides that a personal representative has the same authority over digital assets as the account holder, is an authorized user of the digital asset under computer fraud and unauthorized access laws, and "has the lawful consent of the account holder" to access the digital asset. While UFADAA does make clear that a fiduciary may access a digital asset without criminal liability, UFADAA does not force the provider to disclose electronic communications protected under the SWA. With respect to such protected electronic communications, UFADAA requires only the disclosure of a log of email addresses and certain general data with whom the user communicated. With such data, the fiduciary could potentially obtain the information the fiduciary is seeking from the other party to the electronic communication. For example, if the fiduciary noted on the log provided by the account provider that the account holder frequently received messages from accountstatement@abclifeinsurance.com, the fiduciary could contact abc life insurance to obtain information about the deceased or disabled person's account.

(a) Although it does not force disclosure of protected electronic communications, UFADAA does clarify that a digital asset provider may voluntarily disclose protected electronic communications without liability under the SWA if it chose to do so.

(b) The reason why UFADAA does not compel disclosure of electronic communications protected under the SWA is that such communications could include protected communications of those who have sent messages to the account holder. When compared to non-electronic communications (i.e., letters), this approach seems flawed. After all, if a fiduciary takes possession of a box of letters, the fiduciary may generally read those letters,

even if they were not sent by the deceased or disabled person, without fear of liability. However, the SWA makes this comparison inappropriate, as there is no comparable federal statute, as broad and all-encompassing as the SWA, which protects the privacy of non-electronic communications.

4. A trustee has similar authority over digital assets owned by the trust. Under Delaware's version of UFADAA, an "adviser" has similar authority over digital assets owned by a trust where there is a directed trustee.

5. A guardian or conservator has similar authority over the digital assets of the ward, but only if granted by the court after an opportunity for hearing under the state's guardianship or conservatorship law.

6. An agent acting under a power of attorney has similar authority over the digital assets of the principal, but the agent will have authority to access electronic communications of the principal only if the power of attorney expressly grants this authority. Thus, the power to access and control electronic communications in a power of attorney is a "hot power."

7. UFADAA provides that terms of service that restrict fiduciary access are void as against public policy unless the user, in a manner that is separate from his or her agreement to the other terms of service, expressly indicates a desire to restrict fiduciary access. A provision in a Will restricting fiduciary access would also be honored.

8. State law "shopping" by digital asset providers who do not want to comply with UFADAA is prohibited. UFADAA provides that a choice-of-law provision in a terms of service agreement is unenforceable to the extent that the choice of law would uphold a term of service that restricts fiduciary access.

VI. Planning in the evolving environment

A. First, assess whether the client would like to preserve his digital assets following death or disability. Many clients do not want fiduciaries or anyone to access some or all of their digital assets following death or disability. Many clients do not have a preference, but it is the estate planning attorney's task to inform the client of the repercussions and potential financial and emotional loss that may be suffered if digital assets are not preserved. Many clients do not want their electronic communications (i.e., electronic messages such as email messages, text messages and Facebook messages) available following death or disability, even if they want to preserve other digital assets.

B. If the client does not want his fiduciary to have access, warn the client that, at this time, it may not be possible completely to restrict a fiduciary's access to the client's digital assets following death or disability. Although many digital asset providers currently restrict fiduciary access to digital assets following death or disability, such restrictions may change in future. Many states are enacting legislation such as UFADAA to provide fiduciaries with access to a

deceased or disabled person's digital assets, and such state laws may trump a digital asset provider's restrictions on fiduciary access. It is too soon to tell whether terms of service, estate planning documents and specific disposition instructions that expressly restrict a fiduciary's access to the digital assets will be honored without specific enactment of a statute like UFADAA in the relevant state.

1. Some may view restrictions on access to digital assets following death or disability as contrary to public policy and potentially void, comparing such restrictions to a mandate to "burn the Rembrandt," alluding to the well-known Langbein essay, John H. Langbein, Burn the Rembrandt?: Trust Law's Limits on the Settlor's Power to Direct Trust Investments, 90 B.U. L. REV. 375 (2010). Langbein's essay quotes the Restatement (Third) of Trusts for the poetic principle that it is "capricious to provide that money shall be thrown into the sea, that a field shall be sowed with salt, that a house shall be boarded up and remain unoccupied, or that a wasteful undertaking or activity shall be continued." While the "Burn the Rembrandt" criticism is a legitimate theoretical concern, Langbein points out that the body of case law disallowing destruction of trust property is small. Id., at 377-78.

2. Don't let the perfect be the enemy of the good. For a client that does not want his fiduciary to access electronic communications or other digital assets, consider:

(a) Encouraging client to use only those digital assets that allow the user to clearly specify (in a separate, not "click-through" format) that his data will not be available following death or disability. These authors are currently unaware of any digital asset providers that allow such measures to be taken, however, given where the law is going, it seems that digital asset providers may take these steps in the future.

(b) Including a provision in the estate planning documents providing that the fiduciary shall have no or limited access to digital assets. See, e.g., Appendix A.

(c) Urging client to conduct his digital and online life so that the data that he wants to protect is inaccessible to anyone except himself, both during life and following death or disability.

(i) Sensitive information in the client's inbox and sent mail folders should be deleted frequently.

(ii) Information that needs to be retained can be downloaded to a USB drive or secret cloud storage and highly encrypted before deletion. If a USB drive is used, a back-up USB drive should be kept (USB drives fail from time to time).

(iii) Ensure highly complex usernames and passwords (guess-proof) are being used.

(d) Consider appointing a special digital fiduciary to destroy digital assets following death or disability or specifically bequeathing digital assets to a trusted person for destruction.

C. If the client does want to preserve digital assets, then the appropriate planning method depends on the complexity of the client's digital assets, his technological fluency and his trust of online resources. As with all estate planning, one size does not fit all. It bears repeating that the terms and conditions of certain websites and online-account providers currently prevent anyone other than the user from accessing the user's account, regardless of whether the fiduciary can clearly show he is acting as the user's legal successor and regardless of whether the fiduciary has the user's password. Before the fiduciary attempts to access digital assets, these terms and conditions must be reviewed and the consequences for breach of these terms and conditions discussed with counsel. In most instances, four steps should be taken:

1. Client's significant digital assets of value should be owned by a business entity or trust, if possible. Many digital asset providers recognize the importance of digital assets to a business and will allow an entity to own the digital asset. For example, Southwest Airlines owns and operates a webpage, blog, Twitter account and Facebook page. However, entities usually cannot hold free web-based email accounts or individual social-media accounts.

(a) If the client is a professional athlete, celebrity or public figure who uses social media for endorsements and publicity, the client's management company should own her social-media account. Otherwise, social-media activity can be transferred to company or estate page following death. For example, Dick Clark's Facebook account has been de-activated and turned into a memorial. However, Dick Clark Productions has an active Facebook "fan" page providing press to several charities and businesses.

(b) The terms of service of most digital asset providers that do allow digital assets to be owned by an entity would seemingly also allow such digital assets to be owned by a trust. For example, the terms of service of Twitter do not appear to prohibit a revocable trust from holding a Twitter account. However, because holding digital assets in a trust is not common, it is uncertain how digital asset providers would treat such ownership. Accordingly, these authors recommend that digital assets with substantial value should be placed into a business entity.

2. Create an inventory of digital assets, usernames and passwords. See, e.g., Appendix B (sample questionnaire prompting client to make such a list).

(a) Advantages of using electronic or paper list of digital assets:

(i) Ensures fiduciaries know about valuable digital assets and those digital assets that unlock valuable "hard" assets.

(ii) Easy and inexpensive to implement.

(iii) Easy and inexpensive to update.

(b) Disadvantages:

(i) Must be updated as passwords and digital assets change.

(ii) A reminder to update the digital-asset inventory should be included in the closing instructions of the estate planning engagement (e.g., the client communication where instructions regarding change of beneficiaries, etc. are given). See, e.g., Appendix A.

(c) For clients who have few digital assets, an "old-fashioned" paper list of digital assets, passwords and usernames may be appropriate. This list should be physically secured in a lockbox, safe or locked file cabinet.

(d) The authors' preferred method is to create a password-protected electronic file listing digital assets. The electronic file itself would be stored on the client's home computer or USB drive. Write the password to access the electronic list on a piece of paper that is stored with original estate planning documents or in safe-deposit box.

(e) Electronic list of digital assets should be encrypted, secured with a complex password, and stored appropriately.

(i) Password protecting a MS Word or other Office document can be easily circumvented and is not adequately secure.

(ii) Software packages designed to store confidential documents and passwords such as KeePass, SecuBox or Web Confidential can be helpful.

(iii) Web based services such as Estate Assist or PasswordBox may also be helpful.

(iv) A back-up should be maintained to guard against data loss.

(v) Disclosed password should be changed from time to time.

(vi) The estate planning attorney should not have custody of both the list of digital assets and the password to access the list. Because this information is so valuable, the risk of liability to the attorney is too great.

(vii) If estate planning attorney does not have access to the electronic (or paper) list of digital assets, estate planning attorney can store the password. As with all confidential client information, the attorney has a duty to safeguard this information appropriately and the password should be stored securely to avoid inadvertent or unauthorized disclosure.

3. Counsel the client to select only those digital asset providers that allow the digital asset to be accessed by the fiduciary following death or disability or to be owned by a business entity or trust. Google has recently added an Inactive Account Manager feature that some may find helpful to allow their fiduciaries easier access to their accounts following death or disability. It is available for all Google accounts including, but not limited to, its popular Gmail web-based email service. New and existing Google users can designate up to 10 individuals to receive the contents of the user's Google accounts in the event that such accounts are inactive for a designated period selected by the user. The user may instead choose that the account is deleted after the designated period of inactivity. In the event this feature has not been activated, Gmail may release the contents of the email account (but not the password) to the appropriate fiduciary, although in the authors' experience, it may take them awhile to respond to the fiduciary's request.

4. Add special language to powers of attorney for property, wills, and revocable trusts authorizing fiduciary to access digital assets. See, e.g., Appendix A.

(a) Under current law, the terms of service of a digital asset provider restricting fiduciary access to digital assets currently supersede provisions in an estate planning document expressly authorizing fiduciary access. In other words, these provisions currently have no effectiveness and can be ignored by digital asset providers who refuse to allow fiduciaries to access the deceased or disabled person's digital assets.

(b) However, as discussed above, a number of states have or are in the process of enacting legislation such as UFADAA that authorizes fiduciaries to access digital assets and such laws may trump a provider's terms of service. Some of this proposed legislation grants a fiduciary access to digital assets only if such powers are expressly included in the relevant estate planning document. For example, UFADAA provides that an agent acting under a power of attorney must be specifically authorized by the principal to access the principal's electronic communications.

D. Fiduciary selection: The tech-savvy client should select a fiduciary competent to administer his digital assets, or appoint a special fiduciary to administer digital assets.

1. The fiduciary should be familiar with digital assets and have the technological competency to work effectively with an IT expert, if necessary.

2. If a client has sensitive digital assets/information (for example, an online extramarital relationship), appointment of a special fiduciary may be appropriate.

3. For young clients who appoint their parents or individuals of substantially greater age as fiduciaries, appointment of a contemporary as special fiduciary to deal with social media may be appropriate.

VII. Accessing digital assets of deceased or disabled client

Before the fiduciary accesses a digital asset, he must ensure that he is authorized by the terms of service of the applicable digital asset provider to do so. Accessing digital assets without this authorization can put the fiduciary at risk under federal and most state laws. The next steps to access digital assets when the fiduciary has no inventory of digital assets include:

A. Making a list of all the decedent's known digital assets, including all personal and professional email accounts.

B. After reviewing terms of service of the email provider to determine whether fiduciary access is appropriate, fiduciary should access the decedent's relevant email accounts to search for unknown digital assets and the information relevant to access digital assets (i.e., passwords, security questions, emails sent after the "I forgot my password" button is pressed, etc.). Email is often the gateway to discovering digital assets (and often is the gateway to discovering unknown hard assets), so the client's email account may be a key resource. Email may be accessible from the decedent's home and (if permitted) office computers, tablets, netbooks and smartphone.

1. Internet browser programs can, at the user's option, save username and password information, providing easy access to an email account from a home or work computer.

2. Smartphones and tablets often have direct access to email accounts.

3. If a device is password protected, a software and/or computer forensics specialist may be able to bypass the password.

C. If email account is with an Internet Service Provider (phone or cable company), ISP will often reset the password upon the appropriate fiduciary's request.

D. Web-based email services:

1. As discussed above, Google has been an industry leader in allowing its users to designate up to 10 individuals to receive the contents of the user's Google accounts in the event that such accounts are inactive for a designated period selected by the user.

2. Hotmail may release the contents of the email account (but not the password) to the appropriate fiduciary.

3. Yahoo! will release the contents of the account if the appropriate fiduciary obtains a court order. For example, in 2004, the family of deceased Marine Justin Ellsworth sought to obtain messages from a Yahoo! email account and successfully obtained a court order directing Yahoo! to release the contents of Justin's account. The family was sent a CD containing all messages Justin received, but not sent, as the settings chosen on his email account provided that sent messages would be deleted after a brief period of time (which had passed).

E. Prompt access is extremely important.

1. Important to review or cancel automatic and electronic bill payments. If the estate assets are insufficient to pay all creditors' claims, such automatic payments may expose the fiduciary to liability for paying creditors' claims out of order. Whether insolent or not, unintentional automatic payments may expose the fiduciary to an allegation of waste.

2. If prompt access is not obtained, emails could be deleted: most free email services delete messages if the account has not been accessed for 4 to 9 months and will delete a person's entire account if not accessed for 8 to 12 months.

F. Fiduciary should change the password on all email accounts to a highly complex password to prevent unauthorized access.

G. Fiduciary should access email accounts every week during the period of estate administration.

H. Fiduciary should delete the account after the period of audit on the federal estate tax return (IRS Form 706) is closed or the probate estate has been closed.

I. Fiduciary should check decedent's home and work computers for internet browser history to determine what other digital assets the decedent might have owned.

VIII. Preservation of digital assets

Decide which digital assets, if any, should be preserved and how these assets will be preserved. The following paragraphs address how to best preserve certain types of digital assets.

A. Online Sales Accounts

1. May include online business or sales through eBay, Amazon, Etsy and their related payment entities (e.g., PayPal and Western Union).

2. Timely access to the sales account may be critical to preserve the value of the business and avoid breach of contract actions.

3. Fiduciary should arrange for completion of sales in progress at the time of death, refund incomplete sales and, if desired, prevent future sales from occurring.

4. Most online sales marketplaces will allow the fiduciary to access the decedent's account. However, the fiduciary generally may not transfer the account to another.

B. Webpages and Blogs

1. The decedent's family and friends will likely know if he had a blog or personal webpage.

2. Check credit card statements and email account for evidence of hosting fees.

3. If the decedent paid for web page or blog hosting, usually the fiduciary can have the password reset and can gain full access.

4. Some free services will also reset the password, but ask the decedent's family if or why they desire access to the decedent's blog. In some cases, a copy of the content may suffice.

5. For an online business, contact web-hosting agency to have access transferred to fiduciary.

C. Social Networking Profiles, such as Facebook, LinkedIn ,Twitter, or Myspace

1. Most will not allow fiduciary to access the account of deceased or disabled individual.

2. If decedent is a public figure, prompt access to social networking profiles (if allowed) may be important for endorsement and public relations purposes.

(a) When planning ahead, it is important to review social-media endorsement contract to determine what happens if talent dies unexpectedly.

(b) Casualty insurance may be appropriate to insure against risk of death and resultant breach of endorsement contract.

3. If the fiduciary does not know or cannot guess the password, options include:

(a) Leave the account as is;

(b) Delete the account; or

(c) Turn the account into a memorial page. The account may be used to alert friends and relatives of the decedent's passing.

D. Book, music, movie and other media accounts such as iTunes and Amazon Kindle.

1. Customers own a nontransferable license to use the digital files purchased.

2. According to Amazon's terms of use, "You do not acquire any ownership rights in the software or music content." Cannot be transferred to another (which would include the fiduciary) following death or disability.

3. Apple limits the use of digital files to Apple devices used by the account owner (not successors in interest).

4. Contrast this non-transferability with "old fashioned" printed books and music and movies on disk – one can easily gift or bequeath a physical book, music or movie collection to another. The same is not permitted for electronic book, music or movie collections.

E. When all hope is lost, call a forensic-data expert.

1. While forensic-data experts should be able to find and access most types of digital assets, it is not without great cost (so plan ahead when possible).

2. To recover data effectively, the forensic-data expert may need sensitive personal and financial information about the decedent that the fiduciary may be hesitant to provide.

IX. Valuing digital assets for estate and gift tax purposes

A. Digital assets with financial value should be valued and included on an estate tax return and probate inventory.

B. The IRS is aware that digital assets have value. IRS training materials from 2009 state that agents should:

1. Search the internet to investigate the taxpayer's e-commerce activities;

2. Search the internet archive to view older, archived versions of websites;

3. Identify what domain names are owned by the taxpayer; and

4. Review a taxpayer's business webpage and publicly available social-media profiles.

C. Web-based appraisal services like Web Critiques or Accurate Domains value domain names, websites and online businesses. These services typically review:

1. Recent domain sales

2. Keyword search popularity

3. Brand recognition

4. Search frequency

5. Domain marketability

6. Pay-per-click (PPC) popularity

7. E-commerce value

8. Spoken-word popularity

9. Length of name

10. Suffix

11. Recall value

12. Web frequency

13. Search engine optimization potential

These services are primarily in the business of selling existing web-based businesses, websites and domain names and frequently place unrealistically high values on digital assets. These services are also unfamiliar with methodologies used to value assets for tax purposes.

D. Instead engage business valuation analyst familiar with how to value assets for estate tax purposes and educate him on the unique challenges posed by the valuation of digital assets.

1. The estate tax value of digital assets is the price at which the property would exchange hands between a willing buyer and a willing seller, both with reasonable knowledge of relevant facts.

2. A traditional appraisal may analyze comparable sales, replacement costs, costs to create and future income.

3. Many of these techniques are appropriate for the valuation of digital assets.

E. For a domain name, market-based valuation may be used.

1. Past sales data are available at domain marketplaces such as sedo.com, moniker.com and snapnames.com.

2. However, because each domain name is unique, consideration should also be paid to the items listed in paragraphs C.1-13 above.

F. For a blog, consider whether the death of the blogger renders the asset worthless, making something akin to a key-person discount appropriate.

Appendix A

Sample Provisions Authorizing Fiduciary to Access Digital Assets

Will: My Personal Representative shall have the power and authorization to access, take control of, conduct, continue, or terminate my accounts on any website, including any social networking site, photo sharing site, micro blogging or short message service website or any email service website. All such websites may release my log-on credentials, including username and password, to my Personal Representative, and the website shall be indemnified and held harmless by my estate for any damages, causes of action or claims that may result from this disclosure.

Trust: My Trustee shall have the power to access, handle, distribute, and dispose of digital assets owned by me personally and by this trust, and the power to obtain, access, modify, delete, and control passwords and other electronic credentials associated with digital devices and digital assets owned by me or this trust."

Durable Power of Attorney. The attorney-in-fact shall have (a) the power to access, use, and control my digital devices, to include but not be limited to, desktops, laptops, tablets, storage devices, mobile telephones, smartphones, and any similar digital device which currently exists or may exist as technology develops for the purpose of accessing, modifying, deleting, controlling, or transferring my digital assets, and (b) the power to access, modify, delete, control, and transfer my digital assets, wherever located and to include but not be limited to, my emails received, email accounts, digital music, digital photographs, digital videos, software licenses, social network accounts, file sharing accounts, financial accounts, banking accounts, domain registrations, web hosting accounts, tax preparation service accounts, online stores, affiliate programs, other online accounts, and similar digital items which currently exist or may exist as technology develops, and (c) the power to obtain, access, modify, delete, and control my passwords and other electronic credentials associated with my digital devices and digital assets described above.

Specific Gift in Will/Revocable Living Trust. To the extent I am able to transfer my interests in my digital assets (such assets, wherever located and to include but not be limited to (a) files stored on my digital devices, to include but not be limited to, desktops, laptops, tablets, storage devices, mobile telephones, smartphones, and any similar digital device which currently exists or may exist as technology develops; and (b) emails received, email accounts, digital music, digital photographs, digital videos, software licenses, social network accounts, file sharing accounts, financial accounts, banking accounts, domain registrations, web hosting accounts, tax preparation service accounts, online stores, affiliate programs, other online accounts, and similar digital items which currently exist or may exist as technology develops, regardless of the ownership of the physical device upon which the digital item is stored), to _____.

Sample Provisions Restricting Access to Electronic Communications

Will: Despite any provision herein to the contrary, my Personal Representative shall have no power or authorization to access, view, take control of or terminate any of my electronic communications including any data or information in my email account, social networking

profile, blog or short message service, or any copy of the contents thereof, and any electronic communications service that has custody of my electronic communications is unauthorized to release any of my electronic communications to my Personal Representative or any other person.

Sample Provision in Client Exit Memo Regarding Updating Digital-asset Inventory

As we previously discussed, it may not be possible for your named personal representative and agent to fully access all of your digital property such as online accounts and email. The law on this issue is evolving and we anticipate changes in the near future that will allow your representatives to more fully access your digital property. For this reason, we recommend that you update the inventory of your digital property (which, as you may recall, includes your usernames and passwords) as this information changes. That way, your representatives may access your digital property when the law more readily allows them to do so. Many of our clients also find that it is advantageous to automatically revisit the inventory of digital property every year, since this information can change rapidly.

Appendix B

Digital-asset Inventory

If you have a home computer, smartphone or email account or if you engage in any activities on the internet, please complete the following:

Computer and Phone Information. List all of your personal and professional computers, tablets, netbooks and smartphones and identify the username and password to access each device.

_____

_____

Email Information. List all of your email addresses, describe what activities the email address is used for (e.g., personal, professional or to receive unwanted messages) and indicate the password.

_____

_____

Social Networking Profiles. List the usernames and passwords to each of your social networking profiles such as Linked In, Facebook and Twitter. In the event of your death or disability, should your profile be deleted? If not, who should be responsible for continuing your profile and what would you like for them to do with it?

_____

_____

Blogs, Webpages and Domain Names. List all of your blogs, domain names and webpages and indicate the registrar/host for each. In the event of your death or disability, should these sites be continued? If so, how and by whom?

_____

_____

Online Financial Information. List each bank and brokerage account for which you have online access and indicate your username and password for each account. If you have a paypal or other online purchasing account, list your username and password.

_____

_____

Digital Photos. If you take photos digitally, describe where you store your photos, list any photo sharing websites that you use and indicate your username and password for each site.

_____

_____

Other Online Accounts/Information. List any other online accounts or digital information that may be important or valuable. If relevant, describe what you would like to happen to that account or information if you die or become disabled.

_____

_____

Privacy of Sensitive Information. Is there any sensitive information in the online accounts listed above that should be kept secret from some of your family and friends? If so, how should that information be handled and by whom?

_____

_____