Estate Planning For Digital Assets
Estate Planning Council of Mercer County
June 14, 2017

I. Richard Ploss, JD, CPA, CFP, TEP
Porzio Bromberg & Newman, PC
100 Southgate Parkway
Morristown, NJ 07962
Telephone: 973.889.4087
Email: irploss@pbnlaw.com

Disclaimer: The materials presented in this outline are for education purposes only. Nothing herein should be construed as the rendering of legal advice and these materials should not be relied upon for any controversy before any administrative agency, tribunal or court.

I. INTRODUCTION

(A) This presentation will endeavor to elaborate on the issues and the law surrounding the planning for digital assets that financial (and legal) professionals should consider when assisting clients with their planning for the conservation and disposition of these assets as part of their general estate plan.

(B) Therefore the presentation will focus only on digital asset planning as it relates to individuals and not business and non-business entities.

(C) Definition of a Digital Asset

For purposes of this presentation the term "digital asset" is defined to be any account, document, information, record, photo that is accessible primarily by an individual's access via electronic device (which includes tablets, smart phones, PC computers, Chromebooks, Mac Computers) to the Internet.

(D) Among the items that one would include in the definition of digital asset would be:

(1) Email Accounts

(2) Social Media Accounts (such as Facebook, LinkedIn, Twitter)

(3) Blogs (created and maintained by the individual)

(4) Currency (such as Bitcoins)

(5) Photos and Video posted through web portals to the web

(6) Websites

(7) Online purchasing accounts such as Amazon, PayPal, and catalog accounts

(8) Online store accounts (e.g. EBay, Sirius XM Radio, Pandora, and Spotify)

(9) Music (e.g. iTunes or Google)

(10) Video Sharing Accounts (e.g. YouTube)

(11) Electronic Libraries (such as Kindle, IBooks, Barnes & Noble)

(12) Gaming Accounts

(13) Sports Gambling Accounts (such as Draft Kings and Fan Duel)

(14) Electronic Medical Records (accessible through portals)

(15) Personal Computers. Smartphones and Tablets (which are the portal)[1]

(16) Documents stored to the cloud (through Carbonite, Barracuda, ICloud and Microsoft)

(17) Movie Services (e.g. Netflix and Hulu)

(18) Reward Programs (such as Airline, Credit Card and Hotels)

(19) Contact Lists

(20) Calendars

(21) Text Messages

(22) Electronic Financial Accounts and Account Records

(23) Electronic magazine and newspapers subscriptions

(24) Online Bill Payments offered through banks (automatic payment of monthly bills)

(25) Online sales accounts (e.g. EBay, Craigslist)

(E) Caveat Regarding The Digital Asset Environment

(1) The digital asset arena is a dynamic and growing area of our economy. Technological entrepreneurs are adding new platforms to the digital asset world and change their legal policies with regard to the same on an ongoing basis.

(2) The law has not yet caught up to the digital asset revolution.

(3) Therefore, much of what is discussed in this outline might be and will eventually be obsolete (especially as it relates to some of the social media assets in this presentation).

(4) Be sure to continually read and stay informed.

[1] Note that while a personal computer, tablet, and smartphone are generally considered to be portals to the online digital world, these devices are generally locked down by password or finger touch encryption which results in their being classified as part of the digital world for purposes of this outline.

II. THE LEGAL ENVIRONMENT

(A) Federal Laws

(1) Electronic Communications Privacy Act ("ECPA"): found at 18 U.S.C. §2701 *et. seq.* (also known as the Stored Communications Act). The ECPA contains two prongs relevant to our discussion.

(a) Criminalization: The ECPA makes it a crime for anyone to intentionally access without authorization a facility through which an electronic communication service is provided as well as to intentionally exceed an authorization to access the facility.[2]

(b) Prohibition: The ECPA prohibits an electronic communication service or a remote computing service from knowingly divulging the contents of a communication that is stored by or carried or maintained on that service unless disclosure is made to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient ***or with the lawful consent of the originator or an addressee or intended recipient of such communication or the subscriber in the case of remote computing service***. (Emphasis added) [3]

(2) Computer Fraud and Abuse Act ("CFAA"): found at 18 U.S.C. §1030. This Act protects against anyone who "intentionally" accesses a computer without authorization or exceeds access and imposes criminal liability on the violator.

(a) The U.S. Department of Justice takes the position that it supports a criminal charge when anyone "exceeds authorized access" by violating the access rules set forth in the provider's terms of service agreement. There is no exception for fiduciary access.

(b) Question: Thus if a third person (with access to an individual user's log in credentials and password) accesses the individual user's account without obtaining advance permission from the provider as required under the provider's terms of service agreement - is there a violation of the CFAA?

(c) Question: Does a former employee's access of his/her former employer's computer system constitute a violation of the CFAA?

(i) See United States v. Nosal[4] in which the 9th Circuit US Court of Appeals said "yes."

(ii) But see United States v. Valle[5] (the "Cannibal Cop" Case) in which the 2nd Circuit US Court of Appeals said "no."

[2] See 18 U.S.C. § 2701(a).
[3] See 18 U.S.C. § 2702.
[4] See Nos. 14-10037 & 14-1025 (9th Cir. July 5, 2016).

(B) State Laws

(1) Most states have enacted their own criminal statutes to address the issue of stealing or hacking computers and unauthorized use of a personal or business computer and its data. This outline will not address those laws.

(2) For those who have interest in New Jersey's criminal laws relating to digital assets and computer based information, please see N.J.S. 2C:20-25 (relating to Computer Criminal Activity).

(C) Terms of Service Agreements ("TOSA")

(1) As we are all aware, whenever an individual registers to use and online service or to create online account (or even the use of an app), he or she must generally check a box which signifies that the user is aware of and agrees to the terms of service that govern the use of the website or service. Generally almost no one reads these agreements before checking the box, and no one is quite aware of exactly what they are agreeing to.

(2) Some of the more common traps that exist include:

(a) Automatic termination of the account upon the death of the individual account holder (see Yahoo and LinkedIn for examples of this result).

(b) All property (e.g. photos) transferred to the provider website become the property of the provider and may be used by the provider for whatever purposes it may deem proper.

(c) The records or files (e.g. ITunes music) are non-transferrable at the account holder's death and thus all individual rights terminate at his or her death.[6]

(d) Third parties (such as Personal Representatives of Estates, Agents under Durable Powers of Attorney, Conservators/Guardians) may not access the account.

(e) Legal disputes may only be resolved in a particular forum that may not be convenient to the account holder (for example any disputes involving Facebook or Google must be litigated in the Federal District Court of Northern California - where these entities are headquartered; in Microsoft's case, disputes must be litigated in Federal District Court in Washington State).

[5] See No. 14-2710-CR, 2015 WL 7774548 (2nd Cir. December 3, 2015).
[6] Please ignore family sharing services for purposes of this outline.

III. THE REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT ("RUFADAA")[7]

(A) Brief History

(1) The first iteration of this Act (the Uniform Fiduciary Access to Digital Assets Act or "UFADAA") was promulgated by the Uniform Commissioners in 2012. It was met with opposition by a coalition of internet based businesses and privacy advocates (the "Coalition") who opposed certain provisions. Notwithstanding the opposition, in 2014 Delaware enacted a law regarding digital asset privacy that is substantially similar but not identical to the originally promulgated UFADAA.

(2) The Coalition offered its own version of model legislation with regard to digital assets, which is more limited that the UFADAA and in 2015 Virginia enacted this model legislation.

(3) In 2015 the National Commission on Uniform Laws passed the RUFDAA which provides:

(a) Better coordination with federal privacy laws;

(b) A better definition of the rights and duties of all parties (fiduciaries, internet service providers and digital asset custodians);

(c) A mechanism to give legal effect to an account holder's instructions for the disposition of digital assets.

(4) As of the date of this outline 31 U.S. jurisdictions have enacted the Revised Uniform Fiduciary Access To Digital Assets Act (see more on this below). 13 U.S. jurisdictions (including the District of Columbia) have introduced bills to enact the Revised Uniform Fiduciary Access To Digital Assets Act. 8 U.S. jurisdictions have yet to take action.

(a) States where bills are pending include: Alabama, Alaska, Arkansas, District of Columbia, Georgia, Maine, Missouri, Nevada, New Hampshire, New Jersey, Rhode Island, Texas and West Virginia.

(b) States which currently have not taken any action include, California, Kentucky, Louisiana, Massachusetts, Oklahoma and Pennsylvania (as well Puerto Rico and the Virgin Islands).

(c) For an update of the jurisdictional scorecard please see: http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015)

(5) According to its website (http://www.njleg.state.nj.us/), there are 2 bills pending in the NJ legislature to address the digital asset issue:

[7] Most estate planning lawyers refer to the Act as the "UFADAA" or "FADAA" or "FRADAA Revised"

(a) Assembly Bill No. 3433 which would enact the Uniform Fiduciary Access To Digital Assets Act); and

(b) Assembly Bill No. 3598 which would authorize the Executor or Administrator of a decedent's estate to access the digital assets of a deceased account holder.

(B) RUFADAA Brief Overview of Some Key Provisions

(1) Copy of the RUFADAA may be found and downloaded at www.uniformlaws.org.

(2) The Act is divided into 21 sections.

(3) Section 2 is the definitional section of the Act.

(a) Section 2 (10) defines a "digital asset" to be "an electronic record of which an individual has a right or interest." The comments to the Act state that the following is included in the definition:

(i) Information that is stored on a user's computer and other digital devices;

(ii) Content uploaded onto websites; and,

(iii) Rights in digital property.

Comment: paragraph (c) is somewhat open ended so that implies that items such as bitcoins should be included in the definition.

(b) Section 2(8) defines a "Custodian" to be a person[8] that carries, maintains, processes, retrieves or stores a digital asset of a user.

(c) Section 2(26) defines a "user" to be a person that has an account with a custodian.

(4) Section 3 governs applicability scope of the Act and the fiduciaries who have access to an individual's digital assets. Under Section 3(a), the term "fiduciary" includes the following parties:

(a) An Agent or Attorney-In-Fact acting under a durable power of attorney executed before, on, or after the effective date of the Act;

(b) A Personal Representative (whether under a Will or intestacy) acting for a decedent who died before, on or after the effective date of the Act;

(c) A Court Appointed Conservator (or Guardian) appointed before, on or after the effective date of the Act; and,

[8] Section 2(17) defines a "person" to be "an individual, estate, business or nonprofit entity, public corporation, government or governmental subdivision, agency, or instrumentality, or other legal entity."

(d) A Trustee acting under a trust created before, on, or after the effective date of the Act.

(5) Section 3(c) of the RUFADAA expressly states that the Act does not apply to the digital asset of an employer used by an employee in the ordinary course of the employer's business.

Comment #1: This would signify that a fiduciary would not have access to an employee's company issued laptop computer or smart phone.

Comment #2: What about employers who have a policy in place that allows an employee to "bring your own device" with regard to smartphones? Employers will need to consider either issuing the employee an employer dedicated smartphone (that is truly the property of the employer; or using a phone application ("app") that will enable the employer to delete all employer related data upon termination of employment.

Comment #3: Thus, those of us who are employed by third parties would be advised to be careful about what we store on employer issued phones and computers and ensure that we have our own separate electronic devices in place (which most of us do anyway).

(6) Section 4 provides ways for users to direct the disposition or deletion of their digital assets upon their death or incapacity, and establishes a priority system in the case of conflicting instructions.

(a) First Priority - Online Tool: If the custodian offers an "online tool."[9] a user may direct the custodian via the online tool to disclose to a designated recipient or not to disclose some or all of the user's digital assets, including the content of electronic communications. ***If the online tool allows the user to modify or delete a direction at all times, a direction regarding disclosure using an online tool overrides a contrary direction by the user in a will, trust or power of attorney or other record.***[10] (Emphasis added).[11] [12]

(b) Second Priority - Estate Planning Document or Record: If a user has not used the online tool to give such direction or if the custodian has not provided an

[9] Section 2(16) defines an "online tool" to be "an electronic service provided by a custodian that allows the user, in an agreement distinct from the terms of service agreement between the custodian and user, to provide directions for disclosure or nondisclosure of digital assets to a third person."

[10] Section 2(22) of the Act defines a "record" to be "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." This would imply that a signed written document containing a statement regarding access to the digital asset should suffice. The author would recommend that the document be formally acknowledged to ensure authenticity.

[11] As of the date of this outline the author is aware of two custodians that provides an online tool - Google (see Google Inactive Account Manager at https://www.google.com/settings/account/inactive) and Facebook (see Facebook Legacy Contract feature at https://www.facebook.com/help/660987010672165).

[12] It should also be pointed out that if a custodian grants online tool access to a user's digital account, the user may actually designate a third party individual to be a "designated recipient" to have access to the digital asset. We will not elaborate further on the designated recipient in this outline.

online tool, the user may allow or prohibit in a will, trust, power of attorney, or other record, disclosure to a fiduciary of some or all of the user's digital assets, including the content of electronic communications sent or received by the user.

(c) ***A user's direction by online tool, estate planning document or record overrides a contrary provision in a terms of service agreement that does not require the user to act affirmatively and distinctly from the user's assent to the terms of service.*** (Emphasis added)

Comment #4: Using an online tool for each custodial record can be an overwhelming exercise. Therefore clients should consider some written formally executed document indicating their intent with regard to digital asset disclosure and in states that recognize the doctrine, incorporate the statement by reference into the document.[13] If incorporation by reference is not available, consider using the separate formally acknowledged writing.

Comment #5: If an individual does not utilize an online tool or estate planning document or record, there is a very strong probability that the custodian's TOSA will cover disclosure policy and it is very probable that the custodian will deny the fiduciary access.

(7) Section 6 of the RUFADAA specifically states a custodian may comply with the disclosure requirements in one of the following three manners:

(a) Full Access: by granting the fiduciary full access to the user's digital asset account;

(b) Partial Access: by granting the fiduciary partial access to the user's account sufficient to enable the fiduciary to perform the tasks for which the fiduciary is charged; or,

(c) Copy of Digital Record: by providing the fiduciary with a copy of the digital record on the date on which the custodian received the request for disclosure, which the user could have had access to if the user were alive and fully competent.

Comment #6: Section 6(b) of the RUFADAA allows the custodian to assess a reasonable administrative charge against the fiduciary for making the disclosure (thus there is no such thing as a "free lunch.")

Comment #7: Please note that fiduciary cannot obtain greater access to a user's digital asset accounts than what the user was able to obtain during his/her life while competent.

[13] Please seek legal advice before implementing this strategy. Not all states recognize incorporation by reference.

(8) Section 7 sets forth the rules for disclosure of protected electronic communications of a deceased user.

(a) The Personal Representative of a deceased user's estate must provide the custodian with the following:

(i) a written request for disclosure of the account in physical or electronic form;

(ii) A certified copy of the death certificate of the user;

(iii) A certified copy of the letters of appointment (letters testamentary) of the Personal Representative or a small estate affidavit or a court order;

(iv) Unless the user provided direction using an online tool, then the Personal Representative shall provide the custodian with a copy of the user's Last Will and Testament evidencing the user's consent to disclosure of the electronic communication content.

(9) Sections 9, 10, 11 and 12 basically discuss what content must be provided to a fiduciary under a durable power of attorney, guardianship and trusteeship. Please note that without authorization contained in an online tool or in the governing instrument or court order, the custodian is not obligated to disclose anything.

IV. PRACTICAL POINTS WITH REGARD TO ESTATE PLANNING FOR AND ADMINISTRATION OF DIGITAL ASSETS

(A) The Issues

(1) As a matter of general probate law, the Personal Representative of a Decedent's estate (as well as an Agent under a Financial Durable Power of Attorney and a court appointed Conservator or Guardian) faces two key issues with regard to an individual's digital assets:

(a) Identification Issue: Identifying all of the decedent's/principal's/incapacitated person's digital assets (the "digital estate") at the date of death, incapacity or court appointment.

(b) Marshaling (Access) Issue: Gaining access to the identified digital assets so as to conserve and dispose of them.

(2) This section of the outline will focus on these issues and potential planning that we should consider for our clients (and ourselves). We will also consider potential strategies to resolve the identification and access issues where the planning was not timely completed.

(B) The Identification Issue: Locating the Digital Assets

(1) This is probably the greatest challenge that most Personal Representatives will encounter in the administration process. After all, a Personal Representative cannot effectively administer what he or she does not know exists.

(2) There are three effective methods for dealing with this issue on the planning level (and one could view each method as a separate "generation" in the development of digital asset security):

(a) Method #1 - The Master List: The decedent creates his or her own written or typed "Master List" of digital assets accounts and lists each of the passwords for each so account listed. The list is then printed and stored in an accessible place (perhaps with a trusted third party, the decedent's attorney or accountant, or with the decedent's spouse or family member) for future access. The list can also be available on the decedent's laptop computer.

(i) Advantages:

(A) There is some written record of the decedent's universe of digital assets which can serve as a starting point in the identification process.

(B) If the Master List is kept up to date by the client (i.e. new accounts and passwords documented on the list, updated passwords for existing accounts documented on the list), the identification process is greatly enhanced. If the list is maintained on the decedent's computer (e.g. in the Notepad program on PC's), you will need to make sure that the Executor or family has access to the computer password.

(C) The access process remains "in house" with the decedent and his or her family thereby reducing the risk of theft.

(ii) Disadvantages

(A) Most individuals do not usually do a very good job of updating their Master Lists for new accounts/passwords and updated passwords on updated accounts. Similarly some individuals may terminate their digital asset accounts and never update the Master List for the same.

(B) If the list is stored on a laptop only (i.e. no printout), the possibility always exists that the laptop can go "missing in action" or crash thereby making it very difficult to identify the accounts.[14]

[14] There are obvious ways to reduce this risk - such as purchasing an anti-theft program such as Lo-Jack (which can trace the machine); or in the event of a crash, retaining the services of a computer technician to extract the

(b) Method #2 - Password Manager Programs: Given the proliferation of different passwords for different digital asset accounts,[15] many third party "Password Manager Programs" (such as Dashlane 1Password, mSecure, LastPass, KeePass, RoboForm) have entered the market to provide individuals and selected third parties with access to passwords for digital assets. Some of these programs even generate "strong passwords" for individuals for different websites and provide for automatic login to the digital accounts when the individual accessing the digital asset website. Some of the programs provide for the account holder to grant access to a third person depending upon certain events.

(i) Advantages

(A) If the account holder regularly uses the Password Manager Program for online access, the identification process (and the marshaling process) will be much easier for the Personal Representative of the decedent's estate.

(ii) Disadvantages[16]

(A) If the Password Manager Program is "hacked" by a third party thief, the decedent's digital asset accounts could be at risk.

(B) Determining when to grant a fiduciary access to the Password Manager Program can also be delicate especially if there is a change in nominated fiduciaries.

(c) Commercial Sites:[17]

(i) Digital Estate Planning Services

(A) www.assetlock.net

(B) www.securesafe.com

(C) www.estateplusplus.com

(D) www.passwordbox.com

(E) www.mywonderfullife.com

(F) www.directivecommunications.com

---

information on the hard drive of the computer. But the permutation of issues with this approach can be significant and will not be addressed in this outline.

[15] It is generally recommended that an individual have significantly different passwords for his or her different accounts to negate the effect of a hacker hacking one account and then having access to all accounts.

[16] The author is not making any evaluation or recommendations as to which Password Manager program is best.

[17] Please note that the author has not reviewed the services offered by the providers and some of the service providers may no longer be in business. Nevertheless the domains listed in this section of the outline should provide the reader with a good start in locating planning services.

(ii) Posthumous E-Mail Services

(A) www.bcelebrated.com

(B) www.ifidie.com

(C) www.slightlymorbid.com

(iii) Advantages

(A) Ease of access (if fiduciary has list of instructions)

(iv) Disadvantages

(A) Updating of records

(B) Cost

(d) Also consider utilizing an individual's federal income tax returns; especially in identifying online accounts at online financial institutions which have no brick and mortar presence.

(e) Finally one last source that should be considered is an individual's smartphone as it might be possible to identify digital assets based on the apps that are on the phone (e.g. if one finds the Key Bank online application on a smart phone, one could logically deduce that the individual might have an account at that institution).

(C) The Marshaling (Access) Issue

(1) Each of the above methods, if correctly completed (and updated) should enable the fiduciary to access a user's individual assets.

(2) It would also make sense to include a fully executed and acknowledged record (i.e. statement) indicating that the Personal Representative (or other fiduciary) is to have access to the records.

(3) The biggest problem is ensuring that all digital asset accounts are up to date with regard to identification and passwords.

(D) A Final Issue: What to Do If No Advance Planning has been done?

V. CONCLUSION