Estate Planning for Digital Assets

Presented By:
Shawn C. Snyder, Esq.
Snyder & Snyder, P.A.

March 10, 2022

I. **Estate Planning with Digital Assets**

Every single person living in the modern world is bound to leave a digital trail, whether willingly or unwillingly. That digital trail may include remotely stored emails, business information stored in "the Cloud", family photos on your home computer, iTunes on your phone, NFT's or various forms of crypto currency. Some of these digital assets have real monetary value, while others maybe just sentimental value. As planners, we now have responsibility to make our clients aware of these assets that exist only digitally, and address the issues that are present and unique to the transfer of such assets. Likewise, we are going to be increasingly called to help the fiduciaries that we represent identify, locate, collect and distribute these various assets.

To begin, lets look at some of the most common forms of digital assets. While this list is not exhaustive, it will give us a good point of reference.

Personal Digital Assets

- Personal Emails
- Digital or Online Financial Statements
- Digital Photos
- Social Networking Accounts
- MP3's and iTunes Music
- eBooks
- Game Accounts/ Game Currency
- Dropbox Accounts

Business Related Digital Assets

- Business Emails
- Client Data Stored Offsite (offsite backups)
- Intellectual Property (copyrights, patents, trademarks, etc)
- Domain Names
- Corporate Blogs
- E-Commerce Websites
- Digital Real Estate (Metaverse)

Currency Related Digital Assets

- Bitcoin, Ethereum, Litecoin and various other crypto currency/ coins
- Blockchain ledgers and data
- Online non-convertible currency
- Non-Fungible Tokens (NFT's)

Some of these types of Digital Assets only hold sentimental value, while others assets may be valuable in helping us locate, manage and collect financial assets (such as online personal vaults or e-statements), but there is an ever increasing amount of real monetary

value that is being placed in "convertible" Digital Assets such as crypto currency coins, collectible NFT's, and digital real estate. Here are several examples of where Digital Assets are becoming ever more financially valuable:

A. **Crypto Currencies.** One of the most interesting phenomenons that emerged over the last decade is the creation and use of purely digital currency, often referred to in general as crypto currency. There are over 12,000 crypto currencies in circulation currently, adding almost 1,000 new crypto currencies per month during the first few months of 2022. While it does not exist outside of the digital world (it is both created and maintained digitally in its entirety with no "hard" assets backing it up), the market for this currency is real and increasing, with the price of most crypto currency coins set by what a willing buyer wants to pay to a willing seller. Although the media originally "coined" this currency as primarily a vehicle for funding of illicit transactions with fewer traces, crypto currency has begun to creep into the facilitation of mainstream financial transactions, investment ETF's, retail investor portfolios and even into investable art.

B. **Digital Real Estate.** In 2005, cyber celebrity Jon Jacobs purchased an island of digital real estate in the online game Entropia for $100,000. The ownership of the online real estate allowed him to rent and lease digital land to other players in the game for digital currency that was later convertible into fiat currency, turning his original investment into a stream of income that reached in excess of $100,000 per month at times. Five years later in 2010, Jon sold the rights to the online real estate for $635,000. Think this is a one time event? Its happening again, now in the "Metaverses", on a much grander scale. In a January 2022 interview with *Wired* magazine, Second Life creator Philip Rosedale described the metaverse as a three-dimensional Internet that is populated with live people. While still in its infancy, many large companies, video game producers, and organizations are teaming up to create a network of 3D (or 4D) virtual worlds that invite people to participate in social interactions, entertainment, and business transactions all through their smart phone, computer, or virtual reality headset as if they were live and in person in the world. Many major public companies are racing to purchase and subsequently to develop digital workplaces, retail storefronts, and entertainment venues in metaverse worlds such as Decentraland, Sandbox and Cryptovoxels. A good example of this is the recent actions by investment banking giant JPMorgan Chase, which has set up a retail branch/ shop in the Metajuku mall in the Decentraland metaverse. The bank's lounge features a spiral staircase, a live tiger, and an illuminated portrait of CEO Jamie Dimon. Walmart, Nike, Disney, and Warner Brothers Studios have likewise recently opened metaverse stores, and entertainers like Dua Lipa, Snoop Dogg, and the Red Hot Chilli Peppers are hosting entertainment venues for fans.

C. **Non-Fungible Tokens (aka "NFT's").** NFT's are becoming some of the hottest digital holdings this year. Some are transactional in nature, some are more social in nature, while others are held for investment. But they are one of the least understood digital phenomenon of the more recent digital age. From a basic perspective, an NFT is a digital asset that represents real-world objects like art, music, in-game items and receipts for purchase items. They are usually bought and sold online, frequently with crypto currency, and they are generally encoded with the same underlying software as many crypto currencies, usually on the Etherium blockchain. NFT's have recently been in the news for being sold as art, and recently crypto artist Beeple sold a single piece of NFT artwork through Christies for over $60 Million. However, there are much more common (and less pricey) NFT uses. In 2019 and 2020, the game *Fortnight* was famous for selling digital player clothing, called skins", while other popular games like Roblox sell NFT based avatars, game based currency, an branded merchandise. Likewise, many online retailers are now issuing unique NFT's as a form of digital receipt. Allowing a purchaser to show the NFT as proof of payment upon physical delivery of the item. Finally, in late 2020, the first NFT based real estate "deeds" began surfacing, arguably allowing the transfer of physical real estate via purely digital means.

So the question becomes, as planners, do we ignore these sentimental and sometimes financially valuable assets because they are tough to deal with as a fiduciary, or do we help our clients understand the value of these items and actively plan for the future disposition of such assets?

II. <u>Legal Framework and Limitations</u>

A. Federal Criminal Legislation. The Federal Government enacted the Computer Fraud and Abuse Act (CFAA") in part to criminalize internet theft, data theft, computer hacking, and other forms of internet crime. As written, CFAA criminalizes the ***unauthorized access*** to any computer, online service or online account. Unfortunately, to determine who may and may not access a specific account, even with the explicit permission of the account holder, you must read the service or account provider's Terms of Service contract. As an example, Facebook's Terms of Service Agreement prohibits anyone from logging into a user's Facebook account, other than the user themself, even with the permission of the user. Therefore, a family member, friend, or even a fiduciary that logs into a Facebook account, using the password provided to them by the user themself, has violated the Terms of Service contract and is now committing a federal crime under the CFAA. Fortunately, the Department of justice has made it clear that they are not looking to enforce the CFAA when dealing with simple violations of online Terms of Service contracts, unless there are other more criminal factors involved. However, as advisors to our clients, and to fiduciaries such as Power of Attorneys,

Executors, and Trustees, can we ethically advise clients to access digital assets and accounts where we know that they will be committing a crime under the CFAA? Further, if our fiduciaries do decide to access such accounts and commit a crime, how will we respond to a challenge from an unhappy beneficiary who is aware of the access and its violation of the CFAA?

B. Federal Privacy Legislation. In addition to the criminalization of unauthorized access of digital assets and online accounts, the Federal Government has also passed the Stored Communications Act ("SCA") which creates a right to privacy for data and information stored online. Similar in nature to the federal health information privacy act (often referred to as HIPAA), the SCA creates specific guidelines as to whether, and when, providers of electronic communication services and holders of online data can release the information. As you will see below, these protections can create significant hurdles for family members and fiduciaries who attempt to access information stored online with these service providers and content holders.

1) Law Enforcement Agencies may compel the release of the information otherwise protected by the SCA through the use of subpoenas and other legal procedures.

2) Service providers are prohibited from disclosing information, or granting access to accounts, to non-Law Enforcement individuals (family and fiduciaries), unless one of the statutory exemptions are met. While there are exemptions for specific situations such and employment related emails being released to an employer or being disclosed during a lawsuit against a business, the main exemption that we should be aware of and plan with is the ***"Lawful Consent"*** exemption found in Code Section 2701(b)(3) of the SCA. This exemption allows a service provider to voluntarily turn over (or grant access to) stored information if the recipient has the lawful consent of the creator of such digital asset to access such information. However, this exception only provides that the service provider **MAY** turn over the information, but does not require them to. In fact, there are several national cases where service providers have chosen not to disclose the information. In these situations where the recipient actually had lawful consent, the courts indicated that the SCA exemption does not mandate the disclosure of the stored information, and that the courts could not compel the distribution of the information under the SCA even through legal proceedings.

C. State Criminal Legislation. Every state in the United States has its own version of computer and online fraud statutes that it uses to be able to bring state law charges for online theft, fraud, hacking, and other internet and

computer crimes. In Florida, we have Florida Statute §§ 815.01-815.07 ("Florida Computer Crimes Act" or "Florida CCA"), enacted in 1979, which provides our state legislation. Typical violations under the Florida CCA are

- unauthorized access of another user's account
- unauthorized modification, deletion, copying of files, or programs
- unauthorized modification or damage of computer equipment.

However, Florida-based businesses usually prefer to pursue cases under the federal CFAA for relief because the Florida CCA allows plaintiffs to bring the civil action against a hacker only after a criminal conviction is successful.

D. **State Fiduciary Powers**. Given the lawful consent exemption to the SCA that was discussed above, several states have amended their state statutes to provide that fiduciaries in their state shall be deemed to have lawful consent to access online information under the SCA. This is intended to open the door to allow service providers to voluntarily disclose stored content without the fear of having to determine on a case by case basis whether the fiduciary of an account holder has been given lawful consent.

In 2016, the Florida Fiduciary Access to Digital Assets Act was passed to provide fiduciaries with the ability to access the digital assets of the decedent, principal, ward, or trust, as if the fiduciary were the computer account holder, with some limitations. The act closely follows the proposed law drafted by the Uniform Law Commission. The Act establishes the ability of the digital asset owner, called the "user", to direct disclosure of digital assets and creates the state law rights of a fiduciary to potentially obtain content of electronic communications (not in all situations or all communications), as well as access to all of the user's other digital assets. The result is that an authorized fiduciary will be considered an authorized user for purposes of the state and federal criminal laws prohibiting unauthorized access to electronic accounts.

E. **Website and Service Provider Contracts**. Online service providers mandate that all users agree to the provisions of a Terms of Service Contract ("TOSC's") which governs the actions of both the service provider and the user. Unfortunately, the TOSC's are a take it or leave it situation, and can not be negotiated by the user. Can you imagine if each user could independently negotiate the terms of his or her contract with iTunes or their email service provider? Therefore we are relegated to accepting the often one-sided terms mandated by the service provider. These TOSC's often restrict who may access a registered account or service to the individual that created the account, thereby eliminating any flexibility for fiduciaries or other authorized people from accessing the account. Likewise, such TOS's will usually create

restrictions on the ability of someone other than the user to reset or obtain password. In general, it's the restrictions found in these TOCS's that set up our fiduciaries for potential failure under the CFA and SCA.

III. Practical Problems for Planning and Management

A. **Unawareness**. In order for the fiduciary to take steps necessary to property manage the assets of the estate, the fiduciary has to be aware of those assets' existence.

B. **Digital Bureaucracy**. Many of the companies that serve as custodians of digital media, accounts, and services, have created some form of relief for the fiduciaries and the family members of the deceased. Unfortunately, as each company is acting under the legal restraints and uncertainty still surrounding the digital estate planning, there is no uniformity in approaches chosen by each company, which makes it difficult to find the right approach and navigate through the procedures. The procedures an individual must follow to access the data pertaining to the deceased range from sending a traditional letter with a copy of a death certificate, will, government IDs, personal contact information, proof of relationship, and other verifying information of the deceased, to sending an email with certain information or proof of being appointed a fiduciary, to filling out an online form with no additional verification. Apart from time delay, some of these approaches add a substantial amount of paperwork.

C. **Passwords and PIN Codes.** Passwords are the key to access our many devices and files. Our phones are password protected, our computers and emails are password protected, all of our online financial accounts are password protected, and even now our flash drives can be password protected. Without access to the passwords, the Digital Assets stored in these devices and in these online locations are of reduced if any value.

D. **Encryption.** 32-bit, 64-bit, 128-bit, and 256-bit encryption are all levels of encryption used to further secure locally or remotely saved data, or data that is being transported online from a service provider to your computer or phone. Fiduciaries who are unable to find, guess or otherwise use passwords to open secured accounts are left with the option of trying to break the encryption that secures the digital asset. However, this is easier said than done! As reported by Seagate, a file encryptedwith128-bit AES encryption has over 340,000,000,000,000,000,000,000,000 possible

combinations. To put this into perspective, using today's computer speeds, it would take approximately 200 times the age of our universe to crack a single 128-bit AES encryption, or 70,000,000,000,000,000,000,000,000 years using the entire Bitcoin processing power found worldwide. With this in mind, cracking or guessing a password seems a whole lot more realistic than cracking the encryption. In case you were wondering, it is believed that the current 256 AES encryption (which is stronger than the above referenced 128-bit encryption, will be sufficient encryption protection until approximately the year 2031, when computers will be fast enough that this level of encryption will no longer be strong enough.

IV. **Possible Solutions**

A. Providing Fiduciaries with a Roadmap to the Digital Assets. In order for the fiduciary to take steps necessary to property manage the Digital Assets of the estate, the fiduciary has to be aware of those assets' existence. The first step to an effective transfer of digital assets upon a client's death will be to provide the fiduciary with a "Digital Balance Sheet" that will help the fiduciary locate and understand the nature and extent of the client's digital assets. The following are some general guidelines for types of information to be included on the Digital Balance Sheet:

1) The balance sheet should include physical locations of data, such as location of backup drives, hard drives, disks, computers, laptops, phones, iPads, etc.

2) The balance sheet should provide a list of web addresses or identify other online storage providers where digital records may be kept. This may include social media accounts, email accounts, Dropbox accounts, SkyDrive or other cloud storage services, iTunes accounts, personal financial vaults, etc.

3) The balance sheet should describe the nature and extent of any digital assets such as online credits, digital music or other downloads, domain names that are owned, online bank or bitcoin accounts, digital photos, electronically stored financial records, or other digital assets of monetary or financial value.

4) The balance sheet should list any important expiration dates, renewal dates, due dates, or other critical deadlines to inform the fiduciary of the need to address issues in a timely fashion.

5) Finally, the balance sheet should describe the extent of the financial or sentimental value associated with the items listed on the Digital Balance Sheet.

B. **Digital Will aka "Blogger's Will."** Although not legally enforceable (yet), such document can provide fiduciaries with the ability to understand the scope of the digital assets involved and the steps necessary to property maintain such assets. The contents of the Blogger's Will may vary greatly depending on the asset involved. Likewise, the "Executor" of the Blogger's Will may be someone with a specific knowledge base or skill set, and therefore may be different than the Executor named in a client's traditional estate planning documents. The Blogger's Will should attempt to provide its Executor with Lawful Consent to access stored communications to comply with the SCA exception for disclosure of information. Finally, the Blogger's Will may often provide the executor with passwords, contacts for the hosting websites, advertisers, and contributors, or other information that may be important to help maximize the value of a client's digital assets.

C. **Password Lists.** Many people correctly say that encryption is only as good as its password. Easy passwords allow easy access to encrypted files, while tough passwords, combined with tough encryption, is a recipe for success. But in the case of fiduciaries, this success in protecting data can lead to insurmountable obstacles in accessing digital assets. Therefore, its important to not only leave a roadmap to find the digital assets, but also a list of user names and passwords for each protected asset. While yellow Post-It notes on the computer screen may be easy to find, important passwords should be stored securely. This may be a written list that is located in a home safe or safety deposit box, it may be a online password storage service such as Legacy Locker, RoboForm, Keeper or AfterSteps, or it can be kept on movable storage devices such as IronKey flash drives.

D. **Google's "Inactive Account Manager."** Google and many other large information companies have introduced additional options for Account Settings. For instance, Google's users can "opt-in" to select what will happen with the accounts (including +1s; Blogger; Contacts and Circles; Google Drive; Gmail; Google+ Profiles, Pages and Streams; Picasa Web Albums; Google Voice and YouTube) after the account(s) have been inactive for a certain period of time. At that point, the account can be permanently deleted, but only after a copy of the content has been sent to another user (if any are selected). This effectively allows the fiduciaries to access your data without hitting any legislative roadblocks, as the digital data will be delivered to them automatically at a certain point. Hopefully, many other "big names" in the digital world will follow this lead to allow our clients to deal with digital assets without the legislative lag and uncertainty.

E. **Digital Trusts?** In the tangible world, we often use revocable living trusts to assist with the transfer of traditional assets after a client's passing without having to go through the hassles of probate proceedings. The efficiency of

trusts rely on the concept that a trust entity does not "die" upon the death of its Grantor. Rather, a trust continues to "live" on after the grantor's death. One can't help but wonder if we shouldn't be thinking about using a specialized revocable trust as the "authorized user" on many of our accounts, so that successor trustees could seamlessly step in to manage our digital assets upon our death or disability. Sound promising? Unfortunately the concept is unlikely to work because of the restrictive provisions found in most service provider's TOSC's. Most TOSC's require the user to be a lawful individual (not an entity such as a trust or corporation) thus ruling out the use of trusts as users.

However, as crypto currency, NFT's, and other blockchain held assets become more popular, the concept of digital trusts have become more prevalent as such are not governed by third party TOC's. For an "interesting" take on the use of trusts as an estate planning tool, please see the attached white paper on the Crypoto Currency Inheritance System.

F. **Good Old Fashion Backups of All Digital Data.** We all know that we should backup our computer data regularly, but just like making time to see your estate planning attorney, there is never a good time to do it until its too late. One of the simplest, most efficient, and most cost effective ways to make sure that you Digital Assets are able to be located, accessed and distributed is to keep an up to date backup of all of the data at home. Instead of having to go to Facebook to retrieve digital photos, Dropbox to obtain bank statements, eMoney to find brokerage statements, and Gmail to find your stored emails, a simple regular backup of this data to a hard drive or other accessible storage device would significantly simplify the work of your fiduciaries. Physical access to such device can be provided without violating the CFAA or SCA laws, and a single password will be all that is needed by the fiduciary to be able to collect the majority of the assets. Simple and old fashioned, but effective!

G. **Granting Fiduciaries Legal Powers.** There are a considerable number of arguments being made today that would grant our fiduciaries the right to legally step into the digital shoes of a client once they pass away or become incapacitated. For decades this general concept has been applied with trustees, executors, and power of attorneys for legal and financial decision making. So the question becomes why can't these same fiduciaries that can sell your home, handle investments, and levy lawsuits deal with your Digital Assets? The simple answer is the TOCS that our clients sign when they register for a service says they cant. Period.

As noted above, most states, including Florida, have now attempted to statutorily grant specific fiduciaries the power to either step into the shoes of

the deceased or incapacitated user, or to deem the fiduciary to automatically have lawful consent to access the stored data. These laws, while a step in the right direction, are not uniform and many fall short of solving the problem as service providers are not always ready to accept the powers granted to the fiduciary as such is not statutorily provided for under their local jurisdiction where the TOSC is to be interpreted and enforced. Service providers fear being sued (or at a minimum getting bad publicity) for a breach of their contractual duties and privacy policies if they inappropriately disclose personal data. In fact, violations of such TOCS and privacy policies can lead to FTC penalties, so this is an area where service providers will always take the most conservative approach possible until they are assured that they will not be breaching any duties to their users.

So what are we to do? We do the best we can in this time of legal evolution. First, I pose that as attorneys, accountants, and financial professionals, we should, at a minimum, change the power of attorney, wills and trust forms that we have used for years and add new powers and authorizations to allow the fiduciaries to work efficiently with the digital assets that our clients own. For your reference, I have attached to this outline proposed language that you can implement into your documents, or alternatively provide to your client's attorney with a suggestion that such language be added to their documents. Second, I propose that as a secondary authorization, professionals should suggest to their clients that they sign HIPAA style authorizations that attempt to waive any digital privacy protections, and authorize/ consent to the release of electronically stored information and personal data to fiduciaries. Attached to this outline is a sample copy of such authorization and release. Executing advance authorizations for disclosure and granting fiduciaries specific powers is not guaranteed to work today, as there is little case law or statutory guidance in this area that would mandate that such works. However, clients that have such will be miles ahead of others as this area of the law evolves.

If your asking yourself whether all of the above are needed since Florida has already passed the Act, the answer is maybe... With little case law having made its way to the appellate level Florida courts, we don't how the courts will interpret many aspects of the statute, nor do we know whether companies holding digital materials will voluntarily comply with the statutes. So many practitioners advise a belt and suspenders approach to formally granting powers in the various governing documents, followed up by the general granting of powers in the statute.

*** *The previous information was provided solely for information purposes. An estate plan for an individual may or may not contain the documents and techniques discussed. We highly suggest that you seek the professional advice of a specialist in this field to determine the appropriate estate plan for you or your client's specific situation.* ***

Authorization and Consent for Release of Electronically Stored Information

I, _____, hereby authorize any person or entity that possesses, custodies, or controls any electronically stored information of mine or that provides to me an electronic communication service or remote computing service, whether public or private, to divulge to my then-acting fiduciaries at any time: (1) any electronically stored information of mine, (2) the contents of any communication that is in electronic storage by that service or that is carried or maintained on that service, and (3) any record or other information pertaining to me with respect to that service. The terms used in this authorization are to be construed as broadly as possible, and the term "fiduciaries" includes a guardian or conservator appointed for me, a trustee of my revocable trust, an Attorney in Fact under a valid Power of Attorney, and a Personal Representative (executor) of my estate.

This authorization is to be construed to be my lawful consent under the Electronic Communications Privacy Act of 1986 (which includes the Stored Communications Act), as amended, the Computer Fraud and Abuse Act of 1986, as amended, and any other applicable federal or state data privacy law or criminal law. This authorization is effective immediately. Unless this authorization is revoked by me in writing while I am competent, this authorization continues to be effective during any period that I am incapacitated and continues to be effective after my death.

Unless a person or entity has received actual notice that this authorization has been validly revoked by me, that person or entity receiving this authorization may act in reliance on the presumption that it is valid and unrevoked, and that person or entity is released and held harmless by me, my heirs, legal representatives, successors, and assigns from any loss suffered or liability incurred for acting according to this authorization. A person or entity may accept a copy or facsimile of this original authorization as though it were an original document.

This Authorization and Release shall be interpreted in the broadest sense possible, and shall only augment, and shall not in any way be interpreted to limit, any statutory authority that a fiduciary may have under current or future Florida Statutes.

Dated this _____ day of _____, 2022.

_____

_____
Witness

_____
Witness

Example of Digital Property Provision for a Power of Attorney

Generally the following provision will be inserted as a subparagraph in the section of a Power of Attorney which explicitly enumerates the powers granted to a Attorney in Fact.

Power With Regard to Digital and other Intangible Property.

In the event that I own an interest in any form of electronic, digital or intangible assets (including but not limited to leaseholds, licenses, contractual rights, computing devices, data storage devices, a domain names, user accounts, email accounts, digital pictures, digital music, or any other form of electronically stored information (collectively, "Digital Assets")), then in addition to any other powers granted to my Attorney in Fact under this Durable Power of Attorney, or which may otherwise be provided for under the Florida Statutes, my Attorney in Fact shall have the following powers:

(1) the power to obtain copies of any electronically stored information of mine from any person or entity that possesses, custodies, or controls that information, including but not limited to entities that may be subject to the Stored Communications Act under or similar state laws that may then be in effect;

(2) power to decrypt any encrypted electronically stored information of mine or to bypass, reset, or recover any passwords or other kind of authentication or authorization necessary to gain access to access the Digital Assets;

(3) the power to waive any confidentiality that I may have had under any Terms of Service Agreement or Privacy Policy that I had previously agreed to in regards to any Digital Asset, to the extent allowable under such Terms of Service or Privacy Policy;

(4) the power to access and control the content of any electronic communication of the Principal, whether sent or received by the Principal;

(5) all other powers that an absolute owner of a Digital Asset would have, and any other powers appropriate to achieve the proper investment, management, and distribution of my Digital Assets, including the power to employ any consultants or agents to advise or assist the Attorney in Fact in exercising the powers listed above.

In furtherance of such powers which are granted to the Attorney In Fact above, I hereby authorize, to the extent permitted by federal and state law, including the Electronic Communications Privacy Act of1986 (which includes the Stored Communications Act), as amended, and the Computer Fraud and Abuse Act of 1986, as amended, any person or entity that possesses, custodies, or controls any electronically stored information of mine or that provides to me an electronic communication service or remote computing service, whether public or private, to divulge to my Attorney in Fact (1) any electronically stored information of mine; (2) the contents of any communication that is in electronic storage by that service or that is carried or maintained on that service; and (3) any record or other information pertaining to me with respect to that service. This authorization is to be construed to be my lawful consent under the Stored Communications Act, as amended, and any other applicable federal or state data privacy law or criminal law. The terms used in this paragraph are to be construed as broadly as possible, and the term "user account" includes without limitation an established relationship between a user and a computing device or between a

user and a provider of Internet or other network access, electronic communication services, or remote computing services, whether public or private.

Example of Digital Property Provision for a Will

Generally the following provision will be inserted as a subparagraph in the Powers of Personal Representative (Executor) Section of the Will, and may be modified to be used with Trust Agreements.

Power With Regard to Digital and other Intangible Property.

In the event that at the time of my death I owned an interest in any form of electronic, digital or intangible assets (including but not limited to leaseholds, licenses, contractual rights, computing devices, data storage devices, a domain names, user accounts, email accounts, digital pictures, digital music, or any other form of electronically stored information (collectively, "Digital Assets")), whether included in my probate estate or not, then in addition to any other powers described in this Section or provided for under the Florida Statutes, the powers granted to the Personal Representative of my estate shall include, but not be limited to, the following:

(1) the power to obtain copies of any electronically stored information of mine from any person or entity that possesses, custodies, or controls that information, including but not limited to entities that may be subject to the Stored Communications Act under or similar state laws that may then be in effect;

(2) power to decrypt any encrypted electronically stored information of mine or to bypass, reset, or recover any passwords or other kind of authentication or authorization necessary to gain access to access the Digital Assets;

(3) the power to waive any confidentiality that I may have had under any Terms of Service Agreement or Privacy Policy that I had previously agreed to in regards to any Digital Asset, to the extent allowable under such Terms of Service or Privacy Policy;

(4) all other powers that an absolute owner of a Digital Asset would have, and any other powers appropriate to achieve the proper investment, management, and distribution of my Digital Assets, including the power to employ any consultants or agents to advise or assist the Personal Representative in exercising the powers listed above.

In furtherance of such powers of personal representative, I hereby authorize, to the extent permitted by federal and state law, including the Electronic Communications Privacy Act of1986 (which includes the Stored Communications Act), as amended, the Computer Fraud and Abuse Act of 1986, as amended, any person or entity that possesses, custodies, or controls any electronically stored information of mine or that provides to me an electronic communication service or remote computing service, whether public or private, to divulge to the Personal Representative: (1) any electronically stored information of mine; (2) the contents of any communication that is in electronic storage by that service or that is carried or maintained on that service; and (3) any record or other information pertaining to me with respect to that service. This authorization is to be construed to be my lawful consent under the Stored Communications Act, as amended, and any other applicable federal or state data privacy law or criminal law. The terms used in this paragraph are to be construed as broadly as possible, and the term "user account" includes without limitation an established relationship between a user and a computing device or between a user and a provider of Internet or

other network access, electronic communication services, or remote computing services, whether public or private.