ESTATE PLANNING FOR CYBER PROPERTY – ELECTRONIC COMMUNICATIONS, CRYPTOCURRENCY, NON-FUNGIBLE TOKENS, AND THE METAVERSE



GERRY W. BEYER

Governor Preston E. Smith Regents Professor of Law (Emeritus Pending
Dean's Scholar in Estate Planning
Texas Tech University School of Law

KERRI G. NIPP

Vice President, Fiduciary Officer
Bessemer Trust

SOUTHERN ARIZONA ESTATE PLANNING COUNCIL

October 21, 2026

Tucson, Arizona

© 2026 Gerry W. Beyer & Kerri G. Nipp

revised 10/18/2026

GERRY W. BEYER

Governor Preston E. Smith Regents Professor of Law (Emeritus pending)
Dean's Scholar in Estate Planning
Texas Tech University School of Law
Lubbock, TX 79409-0004
(806) 392-6998
gwb@ProfessorBeyer.com – www.ProfessorBeyer.com

EDUCATION

B.A., Summa Cum Laude, Eastern Michigan University (1976)
J.D., Summa Cum Laude, Ohio State University (1979)
LL.M., University of Illinois (1983)
J.S.D., University of Illinois (1990)

SELECTED PROFESSIONAL ACTIVITIES

Bar memberships: United States Supreme Court, Texas, Ohio (inactive status), Illinois (inactive status)
Member: American Law Institute; American College of Trust and Estate Counsel (Academic Fellow); American Bar Foundation; Texas Bar Foundation; American Bar Association; Texas State Bar Association
Editor-in-Chief, REPTL Reporter, State Bar of Texas (2013-present)
Keeping Current Probate Editor, *Probate and Property* magazine (1992-present)

CAREER HISTORY

Private Practice, Columbus, Ohio (1980)
Instructor of Law, University of Illinois (1980-81)
Professor, St. Mary's University School of Law (1981-2005)
Governor Preston E. Smith Regent's Professor of Law, Texas Tech University School of Law (2005 – 2026)
Visiting Professor, Boston College Law School (1992-93)
Visiting Professor, University of New Mexico School of Law (1995)
Visiting Professor, Southern Methodist University School of Law (1997)
Visiting Professor, Santa Clara University School of Law (1999-2000)
Visiting Professor, La Trobe University School of Law (Melbourne, Australia) (2008 & 2010)
Visiting Professor, The Ohio State University Moritz College of Law (2012)
Visiting Professor (virtual), Boston University School of Law (2014 & 2016)

SELECTED HONORS

Order of the Coif
Isabella Award, National College of Probate Judges (2025)
Distinguished Probate Attorney Lifetime Achievement Award (State Bar of Texas) (2022)
Estate Planning Hall of Fame, National Association of Estate Planners & Councils (2015)
ABA Journal Blawg 100 Hall of Fame (2015)
Outstanding Professor Award (Texas Tech Univ.) (2026) (2016) (2015) (2013) (2010) (2009) (2007) (2006)
Excellence in Writing Awards, American Bar Association, Probate & Property (2024, 2012, 2001, & 1993)
President's Academic Achievement Award, Texas Tech University (2015)
Outstanding Researcher from the School of Law, Texas Tech University (2017 & 2013)
Chancellor's Council Distinguished Teaching Award (Texas Tech University) (2010)
President's Excellence in Teaching Award (Texas Tech University) (2007)
Professor of the Year – Phi Delta Phi (St. Mary's University chapter) (1988) (2005)
Student Bar Association Professor of the Year Award – St. Mary's University (2001-2002) (2002-2003)
Russell W. Galloway Professor of the Year Award – Santa Clara University (2000)
Distinguished Faculty Award – St. Mary's University Alumni Association (1988)
Most Outstanding Third Year Class Professor – St. Mary's University (1982)
State Bar College – Member since 1986

SELECTED PUBLICATIONS

WILLS, TRUSTS, AND ESTATES: EXAMPLES AND EXPLANATIONS (9th ed. 2026); FAT CATS AND LUCKY DOGS – HOW TO LEAVE (SOME OF) YOUR ESTATE TO YOUR PET (2010); TEACHING MATERIALS ON ESTATE PLANNING (5th ed. 2023); 9 & 10 TEXAS LAW OF WILLS (Texas Practice 2026); TEXAS WILLS, TRUSTS AND ESTATES (2nd ed. 2025); 12, 12A, & 12B WEST'S TEXAS FORMS — ADMINISTRATION OF DECEDENTS' ESTATES AND GUARDIANSHIPS (4th ed. 2019); *When You Pass on, Don't Leave the Passwords Behind: Planning for Digital Assets*, PROB. & PROP., Jan./Feb. 2012, at 40; *Wills Contests – Prediction and Prevention*, 4 EST. PLAN. & COMM. PROP. L.J. 1 (2011); *Digital Wills: Has the Time Come for Wills to Join the Digital Revolution?*, 33 OHIO N.U.L. REV. 865 (2007); *Pet Animals: What Happens When Their Humans Die?*, 40 SANTA CLARA L. REV. 617 (2000); *Ante-Mortem Probate: A Viable Alternative*, 43 ARK. L. REV. 131 (1990).

KERRI G. NIPP

Vice President, Fiduciary Officer • Bessemer Trust
300 Crescent Court, Suite 800, Dallas, TX 75201-1800 • (214) 245-1423 • nipp@bessemer.com

PRIOR EXPERIENCE

U.S. Trust, Dallas, TX, *Associate Wealth Strategies Advisor* (August 2016-August 2018)
The Blum Firm, Dallas, TX, *Associate Attorney* (August 2011-July 2016)
Gerry Beyer, Governor Preston E. Smith Regents Professor of Law, Lubbock, TX, *Research Assistant* (March 2010-May 2011)
The Honorable Rory Olsen, Harris County Probate Ct. No. 3, Houston, TX, *Judicial Intern* (2010)

MEMBERSHIPS & DESIGNATIONS

Board certified in Estate Planning and Probate Law by the Texas Board of Legal Specialization
Member of the Digital Assets Committee of the Real Estate, Probate & Trust Law, State Bar of Texas (2014-2017)
Member of the State Bar of Texas Real Estate, Probate, and Trust Law Section
Member of the Dallas Estate Planning Council

EDUCATION

TEXAS TECH UNIVERSITY SCHOOL OF LAW, Lubbock, TX
Doctor of Jurisprudence, *summa cum laude*, Order of the Coif, May 2011
TEXAS TECH ESTATE PLANNING & COMMUNITY PROPERTY LAW JOURNAL, Comment Editor
Dean's List, Fall 2008-Spring 2011; Regent's Scholarship Recipient, Fall 2008-Spring 2011
CALI Excellence for the Future Awards in Guardianship Law; Evidence; Family Law
American Jurisprudence Awards in Commercial Law; Wills & Trusts; Elder Law; Real Estate Finance and Transactions
Tech Law Relay for Life Chairperson, 2009
Women's Caucus, Philanthropy Chairperson, 2009-2010
Tutor for sight-impaired law student, May 2009-May 2010
TEXAS TECH UNIVERSITY, Lubbock, TX
Master of Science in Personal Financial Planning, May 2011
TEXAS TECH UNIVERSITY, Lubbock, TX
Bachelor of Business Administration in Marketing, s*umma cum laude*, December 2007
Graduation Banner Bearer; President's List, Fall 2004-Fall 2007; Robert Amason Outstanding Senior Award, December 2007; Texas Tech Gymnastics, 2004-2007; Tech Marketing Association, 2006-2007

PUBLICATIONS & SPEECHES

"*Estate Planning for Digital Assets*," Wichita Estate Planning Forum, Wichita, Kansas, June 20, 2017.
"*Planning in 2017*," U.S. Trust Attorney Lunch and Learn, Fort Worth, Texas, March 29, 2017.
"*Planning for Corporate Executives*," Wichita Estate Planning Council, Wichita, Kansas, Feb. 14, 2017.
"*Estate Planning for Digital Assets*," State Bar of Texas Advanced Course, Dallas, Texas, June 10, 2015.
"*Estate Planning for Digital Assets*," Midland Memorial Foundation and Midland College Estate Planning Update 2013, Midland, Texas, May 2, 2013.
Gerry W. Beyer & Kerri Griffin, *The Role of Legal Assistants in the Estate Planning Practice*, EST. PLAN. DEV. FOR TEX. PROF., Jan. 2012, at 1.
Gerry W. Beyer & Kerri Griffin, *Estate Planning for Digital Assets*, EST. PLAN. DEV. FOR TEX. PROF., Apr. 2011, at 1.
Gerry W. Beyer & Kerri Griffin, *Lady Bird Deeds: A Primer for the Texas Practitioner*, EST. PLAN. DEV. FOR TEX. PROF., Jan. 2011, at 1.
Kerri M. Griffin, *Safeguarding Against Golden Opportunities*, 2 EST. PLAN. & COMMUNITY PROP. L.J. 441 (2010).

TABLE OF CONTENTS

I. INTRODUCTION 1

II. TYPES OF DIGITAL ASSETS 1

- **A. Personal** 1
- **B. Social Media** 2
- **C. Financial Accounts** 2
- **D. Business Accounts** 2
- **E. Domain Names or Blogs** 2
- **F. Loyalty Program Benefits** 2

III. IMPORTANCE OF PLANNING FOR DIGITAL ASSETS 3

- **A. To Make Things Easier on Executors and Family Members** 3
- **B. To Prevent Identity Theft** 3
- **C. To Prevent Financial Losses to the Estate** 3
- **D. To Avoid Losing the Deceased's Personal Story** 4
- **E. To Prevent Unwanted Secrets from Being Discovered** 5
- **F. To Prepare for an Increasingly Information-Drenched Culture** 5

IV. OBSTACLES TO PLANNING FOR DIGITAL ASSETS 5

- **A. User Agreements** 5
- **B. Federal Law** 6
- **C. Safety Concerns** 8
- **D. Hassle** 8
- **E. Uncertain Reliability of Online Afterlife Management Companies** 8
- **F. Overstatement of the Abilities of Online Afterlife Management Companies** 8

V. BRIEF HISTORY OF FIDUCIARY ACCESS TO DIGITAL ASSETS 8

- **A. Early State Law** 9
- **B. First Attempt at a Uniform Act** 10
- **C. Privacy Expectation Afterlife and Choices Act** 10

VI. REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT 11

- **A. Definitions** 11
- **B. Applicability** 13
- **C. Priority of Instructions** 13
- **D. Disclosure Procedures** 13
- **E. Custodian's Response to Request to Disclose Digital Assets** 16
- **F. Duty and Authority** 17

VII. PLANNING SUGGESTIONS 17
A. Take Advantage of Online Tools 17
B. Back-Up to Tangible Media 17
C. Prepare Comprehensive Inventory of Digital Estate 18
D. Provide Immediate Access to Digital Assets 18
E. Authorize Agent to Access Digital Assets 18
F. Address Digital Assets in a Will 19
G. Place Digital Assets in a Trust 20
H. Use Online Afterlife Company 20

VIII. CRYPTOCURRENCY 20
A. The Basics of Cryptocurrency 21
B. Benefits of Cryptocurrency 22
C. Risks of Cryptocurrency 24
D. Prudent Investment and Fiduciary Concerns 25
E. Taxation and Classification of Cryptocurrency 26
F. Recommendations 27

IX. NON-FUNGIBLE TOKENS 28
A. What is a non-fungible token? 28
B. What do NFTs represent? 29
C. Where are NFTs stored? 29
D. How does a person create an NFT? 29
E. Why does a person create an NFT? 29
F. I still am confused. Are there old-school analogies that may help me understand NFTs? 29
G. What is the value of an NFT? 29
H. What are some examples of notable NFTs? 29
I. Other than collectibles, what are some other possible uses of NFTs? 30
J. How do NFT owners store and access their NFTs? 30
K. What is the first step I need to take regarding NFTs when working with an estate planning client? 30
L. What type of records should a client keep about NFTs? 31
M. Is there a special concern if the client purchases an NFT with cryptocurrency? 31
N. Should the client consider holding NFTs in a business entity? 31
O. How should the client protect the information needed to access NFTs? 31
P. How should a client's will address NFTs? 31
Q. I am a personal representative of a decedent's estate. Can I access the decedent's NFTs? 31
R. I am a personal representative of a decedent's estate. Is there anything special regarding NFTs about which I should be immediately concerned? 32
S. I am a trustee. Can I retain NFTs in a trust or invest in NFTs? 32
T. Are there any religious-based considerations I need to keep in mind with respect to NFTs? 32
U. If I plan on advising clients about NFTs, is there anything else you would recommend that I do? 32

V. If my client mints NFTs, are there any additional special warnings I should provide the client? ..33
W. Why should a charitable organization consider accepting NFT and crypto-currency donations? 33
X. Due to their volatile nature, is it risky for charitable organizations to accept crypto assets? 33
Y. How can a charitable organization accept crypto donations? 33
Z. Are there any additional considerations for organizations wanting to hold on to crypto donations? 33
AA. Are there any specific reporting requirements for crypto donations?.....34
BB. How are crypto assets treated for accounting purposes? 34
CC. Do crypto assets pose any ESG concerns for my organization? 34
DD. Why should my client consider donating crypto assets? 34
EE. How can your client receive a charitable contribution deduction from a crypto donation? 34
FF. What type of crypto assets can be donated?.....35
GG. What are some future issues I may be asked to address about NFTs?.....35

X. METAVERSE ASSETS 35
A. What is the Metaverse?.....35
B. What are some early uses of the Metaverse?.....35
C. How is the Metaverse expanding today? 35
D. Other than gaming assets, what is a common type of Metaverse property? 35
E. How do I address Metaverse assets in a client's estate? 36
F. How do I address Metaverse assets held in trust?.....36

XI. FUTURE REFORM AREAS 36
A. Providers Gather User's Actual Preferences 36
B. Congress Amends Federal Law 36
C. States Enact RUFADAA 36

XII. CONCLUSION 37

APPENDIX A – DIGITAL ESTATE INFORMATION SAMPLE FORM..... 38

APPENDIX B –SAMPLE DOCUMENT LANGUAGE..... 52
A. Wills 52
B. Power of Attorney.....54
C. Authorization and Consent for Release of Electronically Stored Information 54
D. Non-Authorization.....55
E. Pleading 55
F. Court Order.....56

APPENDIX C – SAMPLE REQUEST LETTER TO DIGITAL ASSET CUSTODIAN..... 57

APPENDIX D – A PRIMER FOR PROBATE JUDGES..... 58

APPENDIX E – SUMMARY OF STATE STATUTES..... 61
A. RUFADAA Enacted 61
B. RUFADAA Pending..... 62
C. Non-RUFADAA..... 62

ESTATE PLANNING FOR CYBER PROPERTY – ELECTRONIC COMMUNICATIONS, CRYPTOCURRENCY, NON-FUNGIBLE TOKENS, AND THE METAVERSE

I. INTRODUCTION

For hundreds of years, we have viewed personal property as falling into two major categories – tangible (items you can see or hold) and intangible (items that lack physicality). Recently, a new subdivision of personal property has emerged that many label as "digital assets." There is no real consensus about the property category in which digital assets belong. Some experts say they are intellectual property, some say they are intangible property, and others say they can easily be transformed from one form of personal property to another with the click of a "print" button. *See* Scott Zucker, *Digital Assets: Estate Planning for Online Accounts Becoming Essential (Part II)*, The Zucker Law Firm PLLC (Dec. 16, 2010). In actuality, some accounts that we consider "assets" are simply licenses to use a website's service that generally expire upon death. *See* Steven Maimes, *Understand and Manage Digital Property*, The Trust Advisor Blog (Nov. 20, 2009).

Digital assets may represent a sizeable portion of a client's estate. A survey conducted by McAfee, Inc. revealed that the average perceived value of digital assets for a person living in the United States is $54,722. *McAfee Reveals Average Internet User Has More Than $37,000 in Underprotected 'Digital Assets'*, McAfee.com, (Sept. 27, 2011) (the $37,000 figure is the global average).

This article aims to educate estate planning professionals on the importance of planning for the disposition and administration of digital assets so that fiduciaries can locate, access, protect, and properly dispose of them. The operation of the Revised Uniform Fiduciary Access to Digital Assets Act now enacted in at least forty-three states is explained in detail. Several planning techniques that may be employed are discussed and the appendices include sample forms clients may use to organize their digital assets and sample language that can be used in estate planning documents, court orders, and in request letters to digital asset custodians.

The article also includes coverage of cryptocurrency, non-fungible tokens (NFTs), and metaverse assets.

II. TYPES OF DIGITAL ASSETS

The Revised Uniform Fiduciary Access to Digital Assets Act (hereinafter "RUFADAA") defines "digital asset" as "an electronic record in which an individual has a right or interest. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record." For purposes of this definition, "electronic" means "relating to technology having electrical, digital, magnetic, wireless, optical, electro-magnetic, or similar capabilities," and "record" means "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." RUFADAA § 2.

Digital assets can be classified in numerous different ways, and the types of property and accounts are constantly changing. (A decade ago, who could have imagined the ubiquity of Facebook? Who can imagine what will replace it in the next few decades?) People may accumulate different categories of digital assets: personal, social media, financial, and business. Although there is some overlap, of course, clients may need to make different plans for each type of digital asset.

A. Personal

The first category includes personal assets stored on a computer, tablet, smart phone, or other digital device, as well as uploaded onto a web site or on

a cloud storage account. These can include treasured photographs or videos stored on an individual's hard drive or photo sharing site, such as tinybeans or Flickr. Other examples include emails, texts, documents, music playlists, medical records, tax documents, personal blogs, digital books, on-line gaming or gambling assets, avatars, and recordings from home security systems. The list of what a client could potentially own or control is, almost literally, infinite.

B. Social Media

Social media assets involve interactions with other people with accounts through providers such as Facebook, LinkedIn, Twitter, YouTube, Instagram, Reddit, Tumbler, and Pinterest. These sites are used not only for messaging and social interaction, but they also can serve as storage for documents, photos, videos, and other electronic files.

C. Financial Accounts

The most obvious example of financial digital assets are virtual currencies, which are becoming more prevalent and are addressed in more detail in section VIII below.

Though some bank and investment accounts have no connection to brick-and-mortar buildings, most retain some connection to a physical space. They are, however, increasingly designed to be accessed via the Internet with few, if any, paper records or monthly statements. For example, an individual can maintain an Amazon.com account, have an e-Bay account, be registered with PayPal, and subscribe to online magazines and other media providers.

Many people make extensive arrangements to pay bills online such as income taxes, mortgages, car loans, credit cards, water, gas, telephone, cell phone, cable, and trash disposal. These individuals may not receive traditional paper statements via the U.S. mail with regard to these accounts.

D. Business Accounts

An individual engaged in any type of commercial practice is likely to store some information on computers. Businesses collect data such as customer orders and preferences, home and shipping addresses, credit card data, bank account numbers, and even personal information such as birthdates and the names of family members and friends. Physicians store patient information. eBay sellers have an established presence and reputation. Lawyers might store client files or use a Dropbox.com-type service that allows a legal team spread across the United States to access litigation documents through shared folders.

E. Domain Names or Blogs

A domain name or blog can be valuable, yet access and renewal may only be possible through a password or e-mail.

F. Loyalty Program Benefits

In today's highly competitive business environment, there are numerous options for customers to make the most of their travel and spending habits, especially if they are loyal to particular providers. Airlines have created programs in which frequent flyers accumulate "miles" or "points" they may use towards free or discounted trips. Some credit card companies offer users an opportunity to earn "cash back" on their purchases or accumulate "points" which the cardholder may then use for discounted merchandise, travel, or services. Retail stores often allow shoppers to accumulate benefits including discounts and credit vouchers. Some members of these programs accumulate a staggering amount of points or miles and then die without having "spent" them. For example, there are reports that "members of frequent-flyer programs are holding at least 3.5 trillion in unused miles." *Managing Your Frequent-Flyer Miles* (last visited Aug. 6, 2017). *See also* Becky Yerak, *Online Accounts After Death: Remember Digital Property When Listing Assets*, CHICAGO TRIB., Aug. 26, 2012.

The rules of the loyalty program to which the client belongs plays the key role in determining whether the accrued points may be transferred. Many customer loyalty programs do not allow transfer of accrued points upon death, but as long

as the beneficiary knows the online login information of the member, it may be possible for the remaining benefits to be transferred or redeemed. However, some loyalty programs may view this redemption method as fraudulent or require that certain paperwork be filed before authorizing the redemption of remaining benefits.

III. IMPORTANCE OF PLANNING FOR DIGITAL ASSETS

A. To Make Things Easier on Executors and Family Members

When individuals are prudent about their online lives, they have many different usernames and passwords for their digital assets. Each digital asset may require a different means of access—simply logging onto someone's computer generally requires a password, perhaps a different password for operating system access, and then each of the different files on the computer may require its own password. Each online account is likely to have a username, password, and security questions and answers. Some devices and apps have biometric verification, such as fingerprint scanning, iris recognition, or face recognition. This is the only way to secure identities, but this devotion to protecting sensitive personal information can wreak havoc on families and fiduciaries upon incapacity or death.

Consider the well-publicized "Ellsworth case." After Lance Cpl. Justin Ellsworth was killed in 2004 while serving with the United States Marine Corps in Afghanistan, his parents began a legal battle with Yahoo! to gain access to messages stored in his e-mail account. *Yahoo Will Give Family Slain Marine's E-mail Account*, USA TODAY (April 21, 2005). Yahoo! initially refused the family's request, but ultimately did not fight a probate court order to hand over more than 10,000 pages of e-mails. *Id.* However, the family remained disappointed when the data CD provided by Yahoo! contained only received e-mails and none their late son had written. *Id.* Had Justin provided guidance to his family members regarding his digital assets, his family may have been able to avoid the expense and trouble of going to court, and they also might have gained access to all the emails they desired to have, rather than just some.

In addition, many individuals no longer receive paper statements or bills and instead receive everything via email or by logging on to a service provider's online account. Without instructions from a client, locating, collecting, and monitoring these assets will be a very burdensome task for the client's family members and fiduciaries.

Despite legislation addressing fiduciaries' ability to access and manage digital assets (discussed below), the rights of executors, agents, guardians, and beneficiaries with regard to digital assets are still unclear. The more a client plans in advance for digital assets, the better chance his or her fiduciaries will have to be able to efficiently access and administer such assets.

B. To Prevent Identity Theft

In addition to needing access to online accounts for personal reasons and closing probate, family members need this information quickly so that a deceased's identity is not stolen. Until authorities update their databases regarding a new death, criminals can open credit cards, apply for jobs under a dead person's name, and get state identification cards. A fraud prevention firm by the name of ID Analytics conducted a study in 2012 and found that approximately 2.5 million deceased Americans have their identity stolen each year. *See* Identity Theft and Tax Fraud: Hearing Before the H. Comm. on Ways and Means, 112th Cong. (2012) (statement of Rep. Sam Johnson, Chairman, Subcomm. on Social Security). Criminals know that they have a window of opportunity when someone passes away, so they search through obituaries and other death databases to locate new victims.

C. To Prevent Financial Losses to the Estate

1. Bill Payment and Online Sales

Electronic bills for utilities, loans, insurance, and other expenses need to be discovered quickly and

paid to prevent cancellations. This concern is augmented further if the deceased or incapacitated conducted an online business and is the only person with access to incoming orders, the servers, corporate bank accounts, and employee payroll accounts. *See* Tamara Schweitzer, *Passing on Your Digital Data*, INC., Mar. 1, 2010. Bids for items advertised on eBay may go unanswered and lost forever.

2. Domain Names

The decedent may have registered one or more domain names that have commercial value. If registration of these domain names is not kept current, they can easily be lost to someone waiting to snag the name upon a lapsed registration.

Here is list of some of the most expensive domain names that have been sold in recent years:

1.	AI.com	$70 million	2025
2.	Voice.com	$30 million	2019
3.	360.com	$17 million	2015
4.	Chat.com	$15.5 million	2023
5.	NFTs.com	$15 million	2022
6.	Rocket.com	$14 million	2024
7.	Sex.com	$13 million	2010
8.	Icon.com	$12 million	2025
9.	Telsa.com	$11 million	2014
10.	Hotels.com	$11 million	2001

List of most expensive domain names, Wikipedia (updated Aug. 19, 2026).

3. Encrypted Files

Some digital assets of value may be lost if they cannot be decrypted. Consider the case of Leonard Bernstein who died in 1990 leaving the manuscript for his memoir entitled *Blue Ink* on his computer in a password-protected file. To this day as far as these authors can ascertain, no one has been able to break the password and access what may be a very interesting and valuable document. *See* Helen W. Gunnarsson, *Plan for Administering Your Digital Estate*, 99 ILL. B.J. 71 (2011).

4. Virtual Property

The decedent may have accumulated valuable virtual property for use in on-line games. For example, a planet for the *Entropia Universe* sold for $6 million in 2011 and an asteroid space resort for the same game sold for $635,000 in 2010. Andrea Divirgilio, *Most Expensive Virtual Real Estate Sales*, Bornrich.com (Apr. 23, 2011) (also discussing other high priced sales of virtual property); Oliver Chiang, *Meet The Man Who Just Made a Half Million From the Sale of Virtual Property*, Forbes.com (Nov. 13, 2010). There are also reports of more "reasonable" prices for virtual items such as a virtual sword for use in *Age of Wulin*, a video game, which was sold for $16,000. Katy Steinmetz, *Your Digital Legacy: States Grapple with Protecting Our Data After We Die*, Time Tech (Nov. 29, 2012). If monthly usage or subscription fees apply and are not paid, this virtual property could be lost.

Your client may also have the potential of winning large prizes in videogame tournaments. In 2017, reports indicate that over $100 million in gaming prizes were awarded. *Big Bucks for Pro Gamers*, WIRED, Dec. 2017, at 34.

D. To Avoid Losing the Deceased's Personal Story

Many digital assets are not inherently valuable, but are valuable to family members who extract meaning from what the deceased leaves behind. Historically, people kept special pictures, letters, and journals in shoeboxes or albums for future heirs. Today, this material is stored on computers or online and is often never printed. Personal blogs and Twitter feeds have replaced physical diaries, and e-mails and texts have replaced letters. Without alerting family members that these assets exist, and without telling them how to get access to them, the story of the life of the deceased may be lost forever. This is not only a tragedy for family members, but also possibly for future historians who are losing pieces of history in the digital abyss. Rob Walker, *Cyberspace When You're Dead*, N.Y. TIMES, Jan. 5, 2011.

For more active online lives, this concern may also involve preventing spam from infiltrating a loved

one's website or blog site. Comments from friends and family are normally welcomed, but it is jarring to discover the comment thread gradually infiltrated with links for "cheap Ugg boots." *Id*. "It's like finding a flier for a dry cleaner stuck among flowers on a grave, except that it is much harder to remove." *Id*. In the alternative, family members may decide to delete the deceased's website against the deceased's wishes simply because those wishes were not expressed to the family.

E. To Prevent Unwanted Secrets from Being Discovered

Sometimes people do not want their loved ones discovering private emails, documents, or other electronic material. They may contain hurtful secrets, non-politically correct jokes and stories, or personal rantings. The decedent may have a collection of adult recreational material (porn) which he or she would not want others to know had been accumulated. A professional such as an attorney or physician is likely to have files containing confidential client information. Without designating appropriate people to take care of electronically stored materials, the wrong person may come across this type of information and use it in an inappropriate or embarrassing manner.

F. To Prepare for an Increasingly Information-Drenched Culture

Although the principal concern today appears to be the disposition of social media and e-mail contents, the importance of planning for digital assets will increase each day. Online information will continue to spread out across a growing array of flash drives, iPhones, and cloud accounts, and it will be more difficult to locate and accumulate. As people invest more information about their activities, health, and collective experiences into digital media, the legacies of digital lives grow increasingly important. If a foundation for planning for these assets isn't set today, we may re-learn the lesson the Rosetta Stone once taught us: "there is no present tense that can long survive the fall and rise of languages and modes of recordkeeping." Ken Strutin, *What Happens to Your Digital Life When You Die?*, N.Y. L.J., Jan. 27, 2011 (For fifteen centuries, the meaning of the hieroglyphs on the Rosetta Stone detailing the accomplishments of Ptolemy V were lost when society neglected to safeguard the path to deciphering the writings. A Napoleonic soldier eventually discovered the triptych, enabling society to recover its writings.).

IV. OBSTACLES TO PLANNING FOR DIGITAL ASSETS

Including digital assets in estate plans is a relatively new phenomenon, and there are several obstacles that make it difficult to plan for them. Some of the problem areas include user agreements, federal law, safety issues involved with passwords, the hassle of updating this information, the uncertainty surrounding online afterlife management companies, and the fact that some online afterlife management companies overstate their abilities.

A. User Agreements

1. Terms of Service Agreements ("TOSA")

When an individual signs up for a new online account or service, the process typically requires an agreement to the provider's terms of service. Service providers may have policies on what will happen on the death of an account holder but individuals rarely read the terms of service carefully, if at all. Nonetheless, the user is at least theoretically made aware of these policies before being able to access any service. Anyone who has signed up for an online service has probably clicked on a box next to an "I agree" statement near the bottom of a web page or pop-up window signifying consent to the provider's TOSA. The terms of these "clickwrap" agreements are typically upheld by the courts.

For example, at the end of its TOSA, Yahoo! explicitly states that an account cannot be transferred: "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." *Yahoo! Terms of Service*, Yahoo! (last visited Aug. 6, 2017).

2. Ownership

A problem may also arise if the client does not actually own the digital asset but merely has a license to use that asset while alive. It is unlikely a person can transfer to heirs or beneficiaries music, movies, and books they have purchased in electronic form although they may transfer "old school" physical records (vinyl), CDs, DVDs, books, etc. without difficulty. It has been reported that actor Bruce Willis wants to leave his large iTunes music collection to his children but that Apple's user agreement prohibits him from doing so. *See* Brandon Griggs, *Can Bruce Willis Leave His iTunes Music to His Kids?*, CNN.com (Sept. 4, 2012) and Claudine Wong, *Can Bruce Willis Leave His iTunes Collection to His Children?: Inheritability of Digital Media in the Face of EULAS,* 29 SANTA CLARA COMPUTER & TECH. L.J. 703 (2013). Apple's Terms and Conditions grant the user a license to use their services but expressly prohibit transfers, making it clear that services "are licensed, not sold, to you," and that Apple "grants to you a nontransferable license." Apple Media Services Terms and Conditions (last visited Aug. 6, 2017).

B. Federal Law

There are two primary federal laws that are relevant in the discussion regarding a fiduciary's access to digital assets: (1) the Stored Communications Act ("SCA"), a federal privacy law, and (2) the Computer Fraud and Abuse Act ("CFAA"), a federal criminal law.

1. Stored Communications Act

The Stored Communications Act, 18 USC § 2701 et seq. was enacted in 1986 as part of the Electronic Communications Privacy Act ("ECPA"), 18 USC § 2510 et seq. It regulates access to and disclosure of stored electronic communications and was an effort by Congress to deal with the consequences of online communications upon Fourth Amendment privacy protections. The SCA provides for criminal penalties to be imposed on anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility" and "thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 USC § 2701(a).

In addition, the SCA prohibits an electronic communication service provider or a remote computing service provider from knowingly divulging the contents of a communication that is stored by, carried, or maintained on that service, unless disclosure is made "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." 18 USC § 2702(b)(3).

a. In re Facebook, Inc. ("Daftary case")

The Federal District Court for the Northern District of California applied the SCA in the Daftary case where the personal representative of a decedent's estate attempted to compel Facebook to turn over contents of the decedent's account under the belief that the account held evidence that the decedent did not commit suicide and was instead murdered. *See In re Facebook, Inc.*, 923 F. Supp. 2d 1204 (N.D. Cal. 2012). *See also* James Lamm, *Facebook Blocks Demand for Contents of Deceased User's Account,* Oct. 11, 2012. The court noted that under the SCA, lawful consent to disclosure may *permit* a custodian to disclose electronic communications, but it does not *require* such disclosure, and therefore Facebook could not be compelled to turn over the contents. The court specifically declined to decide whether the personal representatives could provide sufficient "lawful consent" under the SCA, but it also noted that Facebook could determine on its own that the personal representative had standing to consent to disclosure and provide the requested materials voluntarily.

b. Ajemian v. Yahoo!

On October 16, 2017, the Supreme Judicial Court of Massachusetts became the first court to answer the question of whether a personal representative of a deceased individual may grant "lawful consent" on behalf of the deceased individual for purposes of the SCA. *See* Ajemian v. Yahoo!, Inc. In a tremendous win for fiduciaries, the court answered the question in the affirmative, firmly repudiating the position of service providers that the SCA prohibits such disclosure. However, the court's decision echoed the Daftary court's sentiment that even with lawful consent from a personal representative, the SCA does not *require* Yahoo! to disclose the decedent's email account content to the personal representatives; it merely holds that the SCA *permits* the disclosure. The court remanded one portion of the case to the probate court to determine whether the Yahoo! TOSA prevents disclosure. It is anticipated that the probate court, on remand, will issue an order mandating that Yahoo! disclose the contents of the account, now that the Supreme Judicial Court has confirmed that the personal representatives may provide Yahoo! with lawful consent under the SCA.

The United States Supreme Court denied Yahoo!'s petition for a writ of certiorari on March 26, 2018.

2. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 was also enacted by Congress in 1986. It states that anyone who "intentionally accesses a computer without authorization or exceeds authorized access" has committed a crime. 18 USC § 1030(a)(2). A basic violation of the CFAA is a misdemeanor but can become a felony if done for profit or in furtherance of another crime or tort.

The United States Department of Justice asserts that the CFAA allows the government to charge an individual with a crime for violating the CFAA if such individual violates the access rules of a service provider's TOSA. "This position was stated by Richard Downing, Deputy Chief of the DOJ's Computer Crime and Intellectual Property Section, Criminal Division, in testimony presented on November 15, 2011, before the U.S. House Committee on Judiciary, Subcommittee on Crime, Terrorism, and National Security." James Lamm, "*Planning for Digital Property: 'The Future Ain't What it Used to Be' (A Yogi Berra Quote)*," HECKERLING INSTITUTE ON ESTATE PLANNING (2017). However, Mr. Downing also made it clear that the DOJ is not interested in prosecuting minor violations.

3. Interface with User Agreements

Note that both federal statutes described above provide an exception—if an individual has lawful consent or authorization to access an electronic communication (SCA) or a computer (CFAA), that individual is not committing a crime. However, the issue is that most service providers' TOSAs prohibit users from granting anyone else access to their accounts. If the user does not have the ability to give lawful consent, then the person accessing the account is by default exceeding authorized access. Compounding the issue, many providers retain the right to change their TOSAs at any time and without notice to the user. Therefore, a fiduciary's access to an account may be a permitted act one day but become a criminal act the next, just because a service provider makes a change to its TOSA.

Neither the SCA nor the CFAA was intended to address fiduciaries' access to digital assets, but it is easy to see why the statutes have a significant chilling effect on fiduciaries attempting to access certain digital assets. These statutes are complicated, and their application to emails and social networking sites has sparked additional confusion. There have been infinite technological advances since 1986, yet Congress has not updated the statutes to conform to modern technology.

The American College of Trust and Estate Counsel (ACTEC) has drafted language that would fix both of these statutes for estate planning purposes (*see* Letter from Kathleen R. Sherby, ACTEC President 2014-2015, to Jeff Flake, Chairman, Sen. Subcomm. on Privacy, Tech. and the Law, and Darrell Issa, Chairman, H. Subcomm. on Courts, Intellectual Prop. and the

Internet (January 28, 2015). The revisions are simple and include adding a definition to both the SCA and the CFAA, and adding one additional sentence to the SCA.

The problem of fiduciary access possibly being in violation of the law is also an issue in other nations such as the United Kingdom where using a deceased's username and password could result in the person who gains access violating the Computer Misuse Act of 1990. *See* Aileen Entwistle, *Safeguarding Your Online Legacy After You've Gone*, Scotsman.com, March 30, 2013.

C. Safety Concerns

Clients may be hesitant to place all of their usernames, passwords, and other information in one place. We have all been warned, "Never write down your passwords." This document could fall into the hands of the wrong person, leaving your client exposed. With an online afterlife management company or an online password vault, clients may worry that the security system could be breached, leaving them completely exposed. *See* Deborah L. Jacobs, *Six Ways to Store Securely the Keys to Your Online Financial Life*, FORBES, Feb. 15, 2011.

D. Hassle

Planning for digital assets is an unwanted burden. Digital asset information is constantly changing and may be stored on a variety of devices (e.g., desktop computers, laptop computers, smart phones, cameras, iPads, CDs, DVDs, and flashdrives). A client may routinely open new email accounts, new social networking or gaming accounts, or change passwords. Documents with this information must be revised and accounts at online afterlife management companies must be frequently updated. For clients who wish to keep this information in a document, advise them to update the document quarterly and save it to a USB flash drive or in the cloud, making sure that a family member, friend, or attorney knows where to locate it. *See* Tamara Schweitzer, *Passing on Your Digital Data*, INC., Mar. 1, 2010.

E. Uncertain Reliability of Online Afterlife Management Companies

Afterlife management companies come and go; their life is dependent upon the whims and attention spans of their creators and creditors. Lack of sustained existence of all of these companies makes it hard, if not impossible, to determine whether this market will remain viable. Clients may not want to spend money to save digital asset information when they are unsure about the reliability of the companies.

F. Overstatement of the Abilities of Online Afterlife Management Companies

Some of these companies claim they can distribute digital assets to beneficiaries upon your client's death. Clients need to understand that these companies cannot do this legally, and that they need a will to transfer assets, no matter what kind. Using these companies to store information to make the probate process easier could be an effective technique but they cannot be used to avoid probate altogether. David Shulman, an estate planner in Florida, stated that he "would relish the opportunity to represent the surviving spouse of a decedent whose eBay business was 'given away' by Legacy Locker to an online friend in Timbuktu." David Shulman, *Estate Planning for Your Digital Life, or, Why Legacy Locker Is a Big Fat Lawsuit Waiting to Happen*, SOUTH FLORIDA ESTATE PLANNING LAW (Mar. 21, 2009).

V. BRIEF HISTORY OF FIDUCIARY ACCESS TO DIGITAL ASSETS

The rights of executors, administrators, agents, trustees, and guardians to access digital assets of the decedent, principal, beneficiary, or ward has seen rapid development since California first touched on the issue in 2002. This section briefly discusses prior legislation to help place the current majority law, the Revised Uniform Fiduciary Access to Digital Assets Act, into perspective.

A. Early State Law

States began to recognize the need to plan for digital assets and to provide clarity in this area of the law as early as 2002. This legislation took a variety of forms, and can be divided into different "generations."

1. First Generation

The first generation statutes only covered e-mail accounts. They did not contain provisions enabling or permitting access to any other type of digital asset.

California. The first and most primitive first generation statute was enacted by California in 2002, which simply provided, "Unless otherwise permitted by law or contract, any provider of electronic mail service shall provide each customer with notice at least 30 days before permanently terminating the customer's electronic mail address." CAL. BUS. & PROF. CODE § 17538.35 (West 2010). In 2016, California enacted the decedent's estates and trusts provisions of RUFADAA.

Connecticut. Connecticut was one of the first states to address executors' rights to digital assets in 2005 in S.B. 262, requiring "electronic mail providers" to allow executors and administrators "access to or copies of the contents of the electronic mail account" of the deceased, upon showing of the death certificate and a certified copy of the certificate of appointment as executor or administrator, or by court order. S.B. 262, 2005 Leg., Reg. Sess. (Conn. 2005) (codified at CONN. GEN. STAT. ANN § 45a-334a (West 2012)). The bill specifically defined "electronic mail service providers" as "sending or receiving electronic mail" on behalf of end-users. *Id*. In 2016, Connecticut enacted RUFADAA.

Rhode Island. In 2007, Rhode Island passed the Access to Decedents' Electronic Mail Accounts Act, requiring "electronic mail service providers" to provide executors and administrators "access to or copies of the contents of the electronic mail account" of the deceased, upon showing of the death certificate and certificate of appointment as executor or administrator, or by court order. H.B. 5647, 2007 Leg., Jan. Sess. (R.I. 2007) (codified at R.I. GEN. LAWS § 33-27-3 (2012)). In 2019, Rhode Island enacted RUFADAA.

2. Second Generation

Indiana. Perhaps in acknowledgement of changing technological times and the need to address more than just email accounts, Indiana enacted a second generation statute in 2007 which required custodians of records "stored electronically" regarding or for an Indiana-domiciled decedent, to release such records upon request to the personal decedent's personal representative. IND. CODE § 29-1-13-1.1 (2007). This statute has been repealed in Indiana, where RUFADAA took effect on July 1, 2016.

3. Third Generation

Third generation legislation (enacted in Oklahoma, Idaho, Nevada, and Louisiana) acknowledged the changes to the digital asset landscape and expressly recognized social networking and microblogging as digital assets.

Oklahoma. In 2010, Oklahoma enacted legislation with a fairly broad scope, giving executors and administrators "the power . . . to take control of, conduct, continue, or terminate any accounts of a deceased person on any social networking website, any microblogging or short message service website or any e-mail service websites." H.B. 2800, 52nd Leg., 1st Sess. (Okla. 2010) (codified at OKLA. STAT. tit. 58, § 269 (2012)). This law will be replaced by RUFADAA effective November 1, 2024.

Idaho. On March 26, 2012, Idaho amended its Uniform Probate Code to enable personal representatives and conservators to "[t]ake control of, conduct, continue or terminate any accounts of the decedent on any social networking website, any microblogging or short message service website or any e-mail service website." S.B. 1044, 61st Leg., Reg. Sess. (Idaho 2011). Idaho adopted RUFADAA in 2016.

Nevada. In 2013, Nevada enacted Nev. 2013 Sess. Laws ch. 325 authorizing a personal representative to direct the termination of, but not

access to, e-mail, social networking, and similar accounts. Nevada adopted RUFADAA in 2017.

Louisiana. In 2014, Louisiana granted succession representatives the right to obtain access or possession of a decedent's digital accounts within thirty days after receipt of letters. The statute attempts to trump contrary provisions of service agreements by deeming the succession representative to be an authorized user who has the decedent's lawful consent to access and possess the accounts. La. Rev. Stat. § 3191.

B. First Attempt at a Uniform Act

As the years passed, state legislation became increasingly comprehensive, but the laws also became more and more different from one another. The conflicting laws were compounding the issues as questions arose regarding which state's law should apply. The National Conference of Commissioners on Uniform State Laws ("NCCUSL" or "ULC") recognized the need for a uniform act to address fiduciary access to digital assets and to provide uniformity among the states. Many states that were considering legislation stopped in their tracks when the NCCUSL announced it would be drafting a uniform act in 2012.

In the beginning, the NCCUSL was working with representatives of Facebook and industry trade associations to develop the model act, but they parted ways and each started working on a separate model act. The NCCUSL was the first to introduce its act, which it approved as the Uniform Fiduciary Access to Digital Assets Act (UFADAA) on July 29, 2014. The goal of UFADAA was to resolve as many of the impediments to fiduciary access to digital assets to and management of digital assets as possible by reinforcing the notion that the fiduciary steps into the shoes of the accountholder and should be able to do everything with the account that the accountholder could have done.

Delaware was the only state to enact a version of UFADAA. 50 Del Code §§ 5001-5007. Delaware's version of the law was based off of a draft version of the model act prior to it being finalized, but the NCCUSL considered it "close enough" and designated it as an enactment of the model act. After Delaware's enactment, twenty-six other states introduced the act, but it froze in all states due to massive opposition from the technology industry and privacy advocates.

Various online service providers, civil liberties organizations, and state bar sections voiced their concerns about UFADAA to state legislators and governors. Their primary concerns were that UFADAA resulted in an invasion of privacy, it conflicted with the SCA, and it included an improper override of their TOSAs. *See e.g.*, *Joint Letter: Civil Liberty Organizations Respond to the Uniform Fiduciary Access to Digital Assets Act*," Jan. 12, 2015.

C. Privacy Expectation Afterlife and Choices Act

In response to UFADAA, NetChoice, an association of Internet companies that includes Google and Facebook, released its model act entitled the Privacy Expectation Afterlife and Choices Act ("PEAC"). PEAC required "companies to disclose contents only when a court finds that the user is deceased, and that the account in question has been clearly linked to the deceased. Additionally, the request for disclosure must be 'narrowly tailored to effect the purpose of the administration of the estate,' and the executor demonstrates that the information is necessary to resolve the fiscal administration of the estate. And even then, the amount of information is further restricted to the year preceding the date of death. This is stringent guidance meant to protect the privacy of those who communicated with the user while also ensuring that their loved ones can access important financial statements that may be delivered to the account." Alethea Lange, *Everybody Dies: What is Your Digital Legacy?*, Center for Democracy & Technology (Jan. 23, 2015).

A modified version of PEAC was enacted in Virginia effective as of July 1, 2015 (Va. Code Ann. § 64.2-109 et. seq.). (Virginia's version of PEAC was later repealed and replaced by RUFADAA.) It was introduced in California and Oregon, and New York introduced a bill that

incorporated some provisions from PEAC. None of these bills were enacted, and PEAC flat lined as well, primarily due to its inadequacies (it only addressed personal representatives of estates and did not address other fiduciaries) and the fact that it was unworkable for fiduciaries (e.g., requiring personal representatives to get a court order if access was needed). *See* Karin Prangley, *War and PEAC in Digital Assets*, PROB. & PROP., July/Aug. 2015, at 40.

VI. REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT

In response to the overwhelming failure of both model acts, service providers and the NCCUSL entered into negotiations to discuss a compromise. The result was the NCCUSL approving the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) at its July 2015 Annual Conference. This revision is a substantial rewrite with significant changes in presumptions and procedures. "Unlike the original UFADAA, which granted fiduciaries *presumptive* authority to access digital assets, RUFADAA places great emphasis upon whether the deceased or incapacitated user *expressly* consented to the disclosure of the content of the digital assets, either through what RUFADAA refers to as an "online tool" or an express grant of authority in the user's estate planning documents or power of attorney. Hence, RUFADAA respects the concept of "lawful consent" under the SCA, and, unlike UFADAA, does not attempt to impute such lawful consent to the fiduciary." Michael D. Walker, *The New Uniform Digital Assets Law: Estate Planning and Administration in the Information Age*, REAL PROP., TR. & EST. L.J., Spring 2017, at 59.

See also Jeffrey R. Gottlieb, *ULC Rewrites "Uniform Fiduciary Access to Digital Assets Act,"* Plan for the Road Ahead (July 20, 2015).

As of October 18, 2026, RUFADAA has been enacted in forty-seven states, the District of Columbia, and the U.S. Virgin Islands: Alabama, Alaska, Arizona, Arkansas, Colorado, California, Connecticut, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. *See* Uniform Law Commission Enactment Status Map and Appendix D.

As of October 18, 2026, RUFADAA was pending in Massachusetts.

A. Definitions

Section 2 of RUFADAA defines the key terms, the most important of which include:

1. Catalogue of electronic communications.

The "catalogue" includes "information that identifies each person with which a user has had an electronic communication, the time and date of the communication, and the electronic address of the person." RUFADAA § 2(4). For emails, this would include a list of when emails were sent or received and the email addresses involved, but it would not include any of the text of the email or the subject line.

2. Content of an electronic communication.

The "content" includes "information concerning the substance or meaning of the communication which: (A) has been sent or received by a user; (B) is in electronic storage by a custodian . . .; and (C) is not readily accessible to the public." RUFADAA § 2(6). This would include the actual substance or text of an electronic message that is not accessible to the public. If the electronic message was accessible by the public, it would not be subject to the federal privacy protections under the SCA and would not be defined as "content" pursuant to RUFADAA. An example of an electronic communication that would not fall under this definition is a "tweet" by a Twitter user that is accessible to the general public. Michael D. Walker, *The New Uniform Digital Assets Law: Estate Planning and Administration in the*

Information Age, REAL PROP., TR. & EST. L.J., Spring 2017, at 60.

3. Digital Asset

A "digital asset" is defined in RUFADAA as "an electronic record in which an individual has a right or interest. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record." RUFADAA §2(10). "Electronic" means "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities," and "record" means "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." RUFADAA § 2(11) and § 2(22).

The term "digital asset" is a very broad term which encompasses all electronically-stored information, including (a) information stored on a user's computer and other digital devices, (b) content uploaded onto websites, (c) rights in digital property, and (d) records that are either the catalogue or the content of an electronic communication. RUFADAA § 2 cmt.

4. Online Tool

An "online tool" is "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." RUFADAA § 2(16). This "third person" is referred to as the "designated recipient" in RUFADAA to clarify that such a named person is not required to be the fiduciary and is not to be held to the same legal standard of conduct as a fiduciary. *See* RUFADAA § 2 cmt.

Not many service providers offer an online tool. The only three major providers with online tools are Facebook and Google.

Google created its Inactive Account Manager in April 2013 long before any other service provider and long before the promulgation of RUFADAA. The Inactive Account Manager allows users to control what happens to emails, photos, and other documents stored on Google sites such as +1s, Blogger, Contacts and Circles, Drive, Gmail, Google+ Profiles, Pages and Streams, Picasa Web Albums, Google Voice, and YouTube. The user sets a period of time after which the user's account is deemed inactive. Once the period of time runs, Google will notify the individuals the user specified and, if the user so indicated, share data with these users. Alternatively, the user can request that Google delete all contents of the account. *See About Inactive Account Manager*, Google (last visited Aug. 29, 2020).

Facebook, the world's most popular online social network, recognized a need to allow a deceased person's wall to provide a source of comfort in 2009. In its earliest stages, Facebook's deceased user policy allowed for two solutions upon the death of a user: (1) memorialize the account or (2) delete the account. More options are currently available. See *Request to Memorialize or Remove an Account* (last visited Aug. 29, 2020).

The most recent addition to Facebook's deceased user policy is a true online tool to designate a "Legacy Contact," that is, a person designated by a user to delete the account or look after the user's account if it is memorialized. The details of the actions a Legacy Contact can and cannot take are detailed on Facebook's website. See *What data can a legacy contact download from Facebook?* (last visited Aug. 20, 2020).

Apple introduced its Digital Legacy in 2021. This feature, available in iOS 15.2 and later, allows users to designate a trusted contact who can access the user's Apple account data after death. This includes photos, messages, notes, but not sensitive data like payment information or passwords stored in the Keychain.

Users can add a Legacy Contact within their Apple ID settings on their iOS or macOS devices. They can choose one or more Legacy Contacts, and these contacts don't need their own Apple ID or Apple device. An access key is generated when a user adds a Legacy Contact. This key is crucial for access to the data after the user's death. The Legacy Contact can be notified via Messages if

they are also an Apple device user, or they can print out the key or receive it as a PDF.

After the user's death, the Legacy Contact needs to provide a copy of the access key and a death certificate to Apple. Apple will then review the request and, if approved, will create a Legacy Contact Apple ID. Once the Legacy Contact Apple ID is set up, the person can access the deceased user's data. The Legacy Contact has access to the data for a limited time, typically three years from the first approved Legacy Account request. After this period, the account is permanently deleted.

See *How to add a Legacy Contact for Your Apple Account*, Apple.com (Nov. 22, 2024).

More companies will likely soon provide online tool options for users to maintain control over the access to and disposition of their users' accounts.

B. Applicability

Section 3 of RUFADAA addresses access to digital assets for four different types of fiduciaries: (1) a personal representative of a decedent's estate, (2) an agent appointed pursuant to a power of attorney, (3) a conservator or guardian, and (4) a trustee of a trust. Once enacted by a state, RUFADAA applies to these fiduciaries, regardless of whether they were appointed before, on, or after the effective date of the act. However, RUFADAA "does not apply to a digital asset of an employer used by an employee in the ordinary course of the employer's business." For example, a law firm with an internal email communication system is not subject to the act and would not be required to turn over a deceased attorney's emails to the executor of such attorney's estate. RUFADAA § 3.

C. Priority of Instructions

Section 4 of RUFADAA clarifies the priority given to conflicting instructions from a user. First priority is given to online tools. If the online tool allows the user to modify the instructions specified using the online tool at any given time, the instructions provided using the online tool will take first priority.

Second priority is given to the user's instructions in the user's power of attorney, will, trust, or other record.

If the user has not provided instructions through an online tool or written record, then the service provider's TOSA will govern the rights of the user's fiduciaries. If the TOSA does not address fiduciaries' rights (as is often the case), then RUFADAA's default rules will be the only remaining option for the fiduciary. *See* Michael D. Walker, *The New Uniform Digital Assets Law: Estate Planning and Administration in the Information Age*, REAL PROP., TR. & EST. L.J., Spring 2017, at 61.

D. Disclosure Procedures

1. Personal Representatives of Estates

Section 7 and 8 of RUFADAA address disclosure of digital assets to a personal representative of a deceased user's estate, with Section 7 focusing on the disclosure of content of electronic communications and Section 8 focusing on the disclosure of all other digital assets.

a. Contents

If a deceased user consented in the user's will or a court issues a disclosure order, a custodian must disclose the content of an electronic communication to the personal representative of a deceased user's estate if the representative provides:

- a written request for disclosure,
- a certified copy of the deceased user's death certificate,
- a certified copy of letters testamentary or letters of appointment proving the representative's authority, and
- a copy of the documentation (typically, the will) in which the user consented to the disclosure of the content of electronic communications specifically (if not so provided pursuant to an online tool).

In addition, the custodian may request additional information such as:

- information necessary to identify the user's account,
- evidence linking such account to the user, and
- a finding by the court that the account actually belonged to the decedent, the disclosure of the contents would not violate the SCA and other federal laws, the user consented to disclosure, disclosure is permitted by RUFADAA, and disclosure is reasonably necessary for estate administration. RUFADAA § 7.

A sample letter to the custodian of a decedent's digital asset is include in Appendix C.

b. Catalogue and Other Digital Assets

The requirements for a personal representative to gain access to the catalogue and digital assets other than the content of electronic communications are less stringent. Unless prohibited by the user or court order, the personal representative is granted access to the catalogue and digital assets other than the content by default (upon providing the custodian with the specified required documentation, which is basically the same as is required to access contents under 7, except there is no requirement that the decedent's will be produced or that the decedent specifically consented to disclosure).

While § 8 also includes a custodian's ability to request a court order, it does not include a reference "to compliance with the SCA because such non-content disclosures are not prohibited by the SCA." Michael D. Walker, *The New Uniform Digital Assets Law: Estate Planning and Administration in the Information Age*, REAL PROP., TR. & EST. L.J., Spring 2017, at 63.

c. Practical Problems

The ability of a custodian to request a court order under any circumstance makes access very burdensome for personal representatives as well as the courts. One of the authors has heard from representatives of Google and Facebook that they will *always* require a court order. They want the security of a court order before releasing any information for fear of liability for improper disclosure.

The case of In the *Matter of Serrano*, 2017 NY Slip Op 27200 (June 14, 2017) is instructive. A husband requested authority to access his deceased spouse's Google email, contacts, and calendar in order to "be able to inform friends of his passing" and "close any unfinished business, etc." *Id*. New York recently enacted its own version of RUFADAA, so Google, presumably pursuant to such law, requested a finding by the court before making any disclosures to the surviving spouse. *Id*. The court ordered Google to disclose the contacts and calendar information (finding that such items were not contents of electronic communications pursuant to the SCA). *Id*. However, the court stated, "Authority to request from Google disclosure of the content of the decedent's email communications—to the extent petitioner requests such authority—is denied without prejudice to an application by the voluntary administrator . . . establishing that disclosure of that electronic information is reasonably necessary for the administration of the estate." *Id*. While this is not necessarily an unfavorable result for the surviving spouse, it does indicate that custodians may exercise their rights pursuant to RUFADAA to request court orders on a regular basis, which (in this author's opinion) goes against the spirit of RUFADAA.

Another problem is evident from the *Daftary* case discussed above. Courts are likely to be hesitant to make the determination that personal representatives, by sole virtue of having been appointed as fiduciary, can offer "lawful consent" pursuant to the SCA to receive the content of electronic communications.

d. Advice

These concerns emphasize the need for a user to expressly consent to disclosure in the user's estate planning documents or through an online tool. Sample will language is provided in Appendix B.

Because of the likelihood that a custodian will require a court order before granting access, include the appropriate language in the earliest possible pleading in the administration of the

estate of a deceased user. Sample language is provided in Appendix B.

2. Agents Under Powers of Attorney

a. Contents

The rules for agents under powers of attorney are similar to those for personal representatives of decedents' estates. Upon receiving the specified required documentation (a request in written or electronic form, the original or a copy of the power of attorney containing the express consent to disclose, and a certification under perjury that the power of attorney remains in effect) a custodian must disclose to the agent under a power of attorney the contents of electronic communications of the principal user if the user's power of attorney expressly grants the agent authority over such content (unless a court or the user direct otherwise). RUFADAA § 9. Sample power of attorney language is provided in Appendix B.

b. Catalogue and Other Digital Assets

Upon receiving the specified required documentation (basically the same as discussed above for access to contents), a custodian must disclose to the agent under a power of attorney (who has been granted specific authority over digital assets or general authority to act on behalf of the user) the catalogue and digital assets other than the content of the principal user unless otherwise ordered by the court, provided in the power of attorney, or directed by the principal. RUFADAA § 10.

3. Trustees

Sections 11, 12, and 13 of RUFADAA address a trustees' ability to access digital assets, and there are two separate rules depending upon the origination of the digital asset.

a. Trustee is Original User

If the trustee is the original user, meaning that the trustee, in his or her capacity as the trustee, opened an online account or procured a digital asset, the custodian must provide the trustee with all content, catalogues, and digital assets of the trust. RUFADAA § 11.

b. Trustee is Not Original User

If the trustee is not the original user (for example, a settlor has a digital asset and then transfers it to a trust, either during life or at death), then different rules apply whether the trustee is requesting the content or non-content material.

A custodian (upon receiving the specified required documentation, including a certified copy of the trust agreement that grants disclosure of the content specifically and a certification by the trustee under penalty of perjury that the trust exists and the trustee is currently serving as the trustee) must disclose to a trustee the content of electronic communications unless otherwise directed by the user, provided for in the trust agreement, or ordered by the court. RUFADAA § 12.

When the trustee is not the original user, a custodian (upon receiving the specified required documentation) must disclose to a trustee the catalogue and all digital assets other than the content unless otherwise directed by the user, provided for in the trust agreement, or ordered by the court. RUFADAA § 13.

In both cases, the custodian may request additional information such as a number, user name, address, or other unique subscriber or account identifier assigned by the custodian to identify the trust's account or evidence which links the account to the trust.

4. Guardians (Conservators)

The last type of fiduciary covered by RUFADAA is a guardian (conservator) of a protected person. Because a protected person is likely to retain a right to privacy in personal communications, access to digital assets is not automatically granted to a guardian by virtue of the fact that the person is appointed as a guardian. RUFADAA § 14 cmt.

If there is a hearing on the matter, a court may grant a guardian access to the ward's digital assets, that is, the catalogue of electronic communications, and other digital assets in which the ward has a right or interest, but not the contents

of electronic communications. RUFADAA § 14(a).

Without a hearing, a guardian may obtain access to the catalogue and digital assets other than the content of electronic communications but a court order is still required along with other specified required documentation including a certified copy of the court order that granted the guardian authority over the ward's digital assets. RUFADAA § 14(b).

In addition, a guardian may also request that an account be terminated or suspended for good cause upon providing the custodian with a copy of the court order giving the guardian general authority over the protected person's property. RUFADAA § 14(c).

E. Custodian's Response to Request to Disclose Digital Assets

1. Timing

The custodian must comply with a request to disclose not later than sixty days after receipt of a proper request along with the required documentation. RUFADAA § 16(a).

2. Notice to User of Request

The custodian may, but is not required to, notify the user, e.g., the principal or ward, that a fiduciary made a disclosure request. RUFADAA § 16(c). The custodian may properly deny a disclosure request if the custodian is aware of any lawful access to the account following the receipt of the request. RUFADAA § 16(d).

3. Method of Custodian's Disclosure

When a custodian discloses digital assets pursuant to the terms of RUFADAA, the custodian may at its sole discretion:

- grant the fiduciary full access to the user's account,
- limit access to the access that is sufficient for the fiduciary's performance of designated tasks,
- provide the fiduciary with a paper or digital copy of a digital asset,
- assess a reasonable administrative charge for disclosing digital assets,
- withhold an asset deleted by a user, and/or
- make the determination that a request imposes an undue burden on the custodian, and if necessary, petition the court for an order.

RUFADAA § 6.

The NCCUSL acknowledges that each custodian has a different business model, and some may prefer one method for disclosure over another. RUFADAA § 6(a) cmt.

An example of the type of situation NCCUSL is preemptively addressing by allowing the custodian to claim that a request imposes an undue burden is where a fiduciary requests disclosure of "any email pertaining to financial matters," which would require the custodian to sift through all emails and determine which ones were relevant or irrelevant. In such event, the custodian may decline the fiduciary's request, and either the fiduciary or the custodian may request guidance from a court. RUFADAA § 6 cmt.

4. Failure to Disclose

A custodian incurs no penalty for failing to disclose within sixty days of a proper request.

If the custodian does not disclose, the fiduciary may apply to the court for an order directing compliance. RUFADAA § 16(a). The order must state that compliance is not in violation of 18 U.S.C. § 2702. RUFADAA § 16(b). The decedent's estate, principal, ward, or trust bears all the expenses of seeking and obtaining the court order such as attorney fees and court costs.

5. Custodian Protection

A custodian is immune from liability for disclosing or failing to disclose if done in good faith. RUFADAA § 16(f). However, a custodian is likely to be liable if it fails to comply with a valid court order. RUFADAA § 16 cmt.

F. Duty and Authority

Section 15 specifies the nature, extent, and limitation of the fiduciary's authority over digital assets. RUFADAA § 15 cmt. Among other things, it specifically states that fiduciaries managing digital assets are subject to the fiduciary duties of care, loyalty, and confidentiality. It also specifies that a fiduciary acting within the scope of the fiduciary's duties is an authorized user for purposes of applicable computer fraud and unauthorized computer access laws. RUFADAA § 15.

VII. PLANNING SUGGESTIONS

Legal uncertainty reinforces the importance of planning to increase the likelihood that an individual's wishes concerning the disposition of digital assets will be actually carried out. Even individuals who believe it is important to plan for digital assets are not taking steps to plan for them. *See* Becky Yerak, *Online Accounts After Death: Remember Digital Property When Listing Assets*, CHICAGO TRIB., Aug. 26, 2012. (reporting that a survey by BMO Retirement Institute revealed that 57% of respondents who believed it was very or somewhat important to plan for digital assets had not made such plans).

Despite the fact that states are addressing the issues surrounding fiduciary access to digital assets for over a decade, many attorneys opted to wait and see what would happen in their states before attempting to help their clients plan for digital assets. If the desire to help clients is not enough to motivate attorneys to begin addressing these issues, perhaps the fear of violating the rules of professional conduct will. ABA Model Rule 1.1 states, "A lawyer shall provide competent representation to a client." The ABA added a new comment 8 to Model Rule 1.1 that states, "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . . ." Attorneys should be aware of the challenges digital assets impose on clients and their appointed fiduciaries, and these challenges need to be discussed with clients as part of competent representation. "We all know the old adage that, 'ignorance of the law is no excuse.' The ABA is telling us that 'ignorance of technology is no excuse.'" James Lamm, "*Planning for Digital Property: 'The Future Ain't What it Used to Be' (A Yogi Berra Quote)*," HECKERLING INSTITUTE ON ESTATE PLANNING (2017).

With almost all states enacting RUFADAA, and with RUFADAA's emphasis on respecting an accountholder's intent as evidenced through online tools and planning documents, the best advice we can give to clients is to be proactive, make their wishes known, and stop dismissing digital assets as something inconsequential.

A. Take Advantage of Online Tools

As previously mentioned, most service providers do not currently provide an online tool option to their users such as Google's Inactive Account Manager, Facebook's Legacy Contact, and Apple's Legacy Contact. However, because so many states are enacting RUFADAA, combined with the fact that RUFADAA allows the service providers to maintain control over fiduciary access to and management of their users' accounts by creating an online tool option, we will most likely start to see more service providers creating online tools.

Clients should utilize the online tool option whenever it is available. In a state that has enacted RUFADAA, if the client has the ability to change his or her directions pursuant to the online tool at any time, the client's instructions using the online tool will trump any other document or agreement and will be the controlling instructions for that account.

B. Back-Up to Tangible Media

Clients should consider making copies of materials stored on Internet sites or "inside" of devices on to tangible media of some type such as a CD, DVD, portable hard drive, or flash drive. The client can store these materials in a safe place, such as a safe deposit box, and then leave them directly to named beneficiaries in the user's will. Of course, this plan requires constant updating and

may remove a level of security if the files on these media are unencrypted. However, for some files such as many years of vacation and family photos, this technique may be effective.

C. Prepare Comprehensive Inventory of Digital Estate

1. Creation

Each client should prepare a comprehensive audit of his or her digital world, including a list of how and where digital assets are held, along with usernames, passwords, answers to "secret" questions, and what he or she would want to happen to each account in the event of disability or death. Sample forms are included in Appendix A. Such an inventory will help fiduciaries locate and collect digital assets. Once this inventory is created, it is just as important for clients to make sure they keep it updated when they change passwords, open new accounts, etc. Lawyers can motivate clients to create such a digital inventory by informing them what happens in the absence of planning, the default system of patchwork laws and patchy service provider policies, as well as the choices for opting out of the default systems.

2. Storage

As addressed earlier, there is a safety concern involved with this approach to planning. Careful storage of the inventory document is essential. Giving a family member or friend this information while alive and well can backfire on your clients. For example, if a client gives his daughter his online banking information to pay his bills while he is sick, siblings may accuse her of misusing the funds. Further, a dishonest family member would be able to steal your client's money undetected.

If you decide that a separate document with digital asset information is the best route for your client, this document could be kept with your client's will and durable power of attorney in a safe place. The document can be delivered to the client's executor upon the client's death or agent upon the client's incapacity. Clients can take extra steps to protect this information, such as by encrypting this document and keeping the passcode in a separate location as a further safeguard. Another option is to create two documents; one with part of the needed information, such as usernames, and one with the rest of the information, such as passwords. The documents can be stored in different locations or given to different individuals.

A newer option is to use an online password storage service such as 1Password, KeePass, or my-iWallet. Your client would then need to pass along only one password to a personal representative or agent. *See* Nancy Anderson, *You Just Locked Out Your Executor and Made Your Estate Planning a Monumental Hassle*, FORBES, Oct. 18, 2012. However, this makes this one password extremely powerful as now just one "key" unlocks the door to your client's entire digital world.

Warning: Giving someone else the client's user name and password may be against the TOSA. Accordingly, if someone uses your client's access information, it may be deemed a state or federal crime because it exceeds the access to that information that is stated in the user agreement.

D. Provide Immediate Access to Digital Assets

Your client may be willing to provide family members and friends immediate access to some digital assets while still alive. Your client may store family photographs and videos on websites such as Flickr, GoogleDocs, DropBox, Shutterfly, and DropShot which permit multiple individuals to have access. Your client could create a family YouTube channel by using a password to privately protect the videos. *See* Nancy Anderson, *You Just Locked Out Your Executor and Made Your Estate Planning a Monumental Hassle*, FORBES, Oct. 18, 2012.

E. Authorize Agent to Access Digital Assets

If your state has adopted RUFADAA, a broadly drafted power of attorney should provide the agent with power over the catalogue and digital assets other than the content of electronic communications, but it will not provide power over the content unless the power of attorney specifically provides that the agent should have access to the content. The power of attorney

document must specifically reference access to the content of electronic communications. Sample language is included in Appendix B that should give the agent access all digital assets and their contents.

Some statutory power of attorney forms have been amended to make it easy for a principal to authorize the agent to access digital assets and their contents. TEX. EST. CODE § 752.051.

Also note that if you have a very private client who does not want his agent to have access to any digital assets, this should be specifically stated in his power of attorney. Otherwise, the agent might be granted access.

F. Address Digital Assets in a Will

Keep in mind that a will becomes public record once admitted to probate, so placing security codes and passwords within it is not recommended. Further, amending a will each time a testator changes a password would be cumbersome and expensive. While a will is not an appropriate place for passwords and security codes, there are several places within a will where it might make sense to address digital assets.

1. Disposition of Digital Assets

Many of the digital assets that we "buy" and think we "own" are not transferable upon death or are simply licenses to use the digital asset during life. However, some digital assets may be transferable, so wishes with regard to disposition should be made clear, just in case those wishes can be followed. If a transferable digital asset is not specifically gifted, it will pass via the residuary clause which could cause the asset to pass in undivided shares to multiple beneficiaries causing considerable difficulty with management and division.

Furthermore, at least one commentator has focused "on the troubling implications of contracts limiting the right to devise digital assets" and "argues that users of digital assets, in light of our theories and methodologies used to define property, have property interests that allow a user to determine how an account should be treated upon his or her death." Natalie M. Banta, *Property Interests in Digital Assets: The Rise of Digital Feudalism*, CARDOZO L. REV., 2017, at 1102. It is possible that users may one day have more control over the disposition of their digital assets than they do today.

It is also important to note that if the ownership of the digital asset upon death is governed by the TOSA, the asset may actually be of the non-probate variety. Thus, like a multiple-party bank account or life insurance policy, the digital asset may pass outside of the probate process.

2. Personal Representative Access to Digital Assets

Digital assets should also be addressed in a will in the personal representative's powers section, which is where RUFADAA comes into play. If your state has enacted RUFADAA, the fiduciary should be able to get access to the catalogue and digital assets other than the content of electronic communications without any special language in the will, but the fiduciary will only be able to access the content if the will (or other record) specifically grants the fiduciary access to such content. All wills should now include provisions making it clear whether the testator intends for the fiduciary to have access to some or all digital assets.

A growing trend is to recommend that the testator include the e-mail addresses of the accounts to which the testator wants to grant access. This helps courts and providers to associate the e-mail addresses with the testator because many people use e-mail addresses that are not obviously connected the person's names.

Appendix B includes sample provisions that may be used in a will (or adapted for use in a revocable trust). Appendix B also includes a sample "Authorization and Consent for Release of Electronically Stored Information" that should qualify as an "other record" under RUFADAA. *See* RUFADAA § 7.

3. Other Digital Asset Concerns

It may be prudent to address digital assets in the definitions section of a will. A broad definition of digital assets is preferable, such as the compilation of RUFADAA definitions provided at the beginning of this outline. *See* RUFADAA § 2(10), (11), and (22).

There are other things clients can do in their wills. For example, you could specifically reference within the will that there is a digital asset inventory that lists usernames and passwords and provides the fiduciary with the testator's desires for each account. This would alert the fiduciary that such a resource is available and needs to be located.

If a client has substantial digital assets or thinks that someone with special skills needs to be appointed to manage the digital assets, the client may consider appointing a separate fiduciary to handle just the digital assets or request that the personal representative hire a digital asset manager to help.

G. Place Digital Assets in a Trust

One of the most innovative solutions for dealing with digital assets is to create a revocable trust to hold the assets. *See* Joseph M. Mentrek, *Estate Planning in a Digital World*, 19 Ohio Prob. L.J. 195 (May/June 2009). A trust may be a more desirable place for account information than a will because it would not become part of the public record and is easier to amend than a will.

Recall that under RUFADAA, if the user originates an account within a trust, the trustee should have complete access to the catalogue and all digital assets, including the content of electronic communications. *See* RUFADAA § 11. If the account is not originated within a trust, and assuming the asset is transferable, the user could transfer it into a trust, and then RUFADAA §§ 12 and 13 would be applicable to the trustee's management authority. The trust agreement could provide the trustee with detailed instructions regarding management and disposition. *See* Jessica Bozarth, *Copyrights & Creditors: What Will Be Left of the King of Pop's Legacy?*, 29 CARDOZO ARTS & ENT. L.J. 85, 104-07 (2011).

Furthermore, it is possible that by placing the assets in a trust, a user might enable licenses to survive beyond the death of the user if the trust owns these accounts and assets instead of an individual, defeating a TOSA that specifies otherwise. When a person accumulates more digital assets, designating these assets as trust assets may be as simple as adding the word "trustee" after the owner's last name. *See* John Conner, *Digital Life After Death: The Issue of Planning for a Person's Digital Assets After Death*, 4 EST. PLAN. & COMM. PROP. L.J. 301 (2011).

However, creating a separate revocable trust for digital assets may be overkill for many individuals and only be practical for those with digital assets of substantial value.

H. Use Online Afterlife Company

Entrepreneurs recognizing the need for digital estate planning have created companies that offer services to assist in planning for digital assets. These companies offer a variety of services to assist clients in storing information about digital assets as well as notes and emails that clients wish to send post-mortem. As an estate planning attorney, you may find this additional service to be valuable and recommend one to your clients. Your client must use due diligence in investigating and selecting a digital afterlife company.

VIII. CRYPTOCURRENCY

Less than a decade ago, if an estate planner asked clients whether they owned any cryptocurrency, the most likely response would be, "You mean, money to buy a crypt?" Now, due to the widespread media coverage of Bitcoin, the most famous of all cryptocurrencies, most clients will have some basic idea about what the estate planner is inquiring.

The use of cryptocurrency is increasing at a rapid pace. As of October 2026 there were over 20 million Bitcoins in circulation worth over $1.6 trillion. *See* Blockchain, *Bitcoins in Circulation*. Although only a few cryptocurrencies in addition to Bitcoin are well-known outside the

cryptocurrency community (e.g., XRP, Ethereum, EOS, and Stellar), over 2,400 different virtual currencies are actively traded. *See* CoinMarketCap, *Top 100 Cryptocurrencies by Market Capitalization*. These other cryptocurrencies are sometimes referred to as *altcoins*, meaning that they are an alternative to Bitcoin.

A recent survey revealed that 25% of individuals between the ages of 24 and 38 who either had $50,000 of investable assets or earned $100,000 or more per year own cryptocurrency. *See* Megan Henney, *More Rich Millennials are Investing in Cryptocurrencies*, Foxbusiness.com (Nov. 1, 2018). A growing number of mainstream businesses already accept Bitcoin such as Microsoft, Subway, KFC Canada, many Etsy vendors, Overstock.com, Whole Foods, Dish Network, AT&T, and Expedia. *See* Jonas Chokun, *Who Accepts Bitcoins* (listing approximately 100 vendors who accept Bitcoins). In addition, some law firms are already accepting Bitcoin in payment of legal services.

This section starts by building a basic foundation about virtual currencies and how they operate. The section then reviews the estate planning and administration issues that arise with owning cryptocurrency and concludes with recommendations for how to address virtual currency in your practice.

A. The Basics of Cryptocurrency

Before looking at cryptocurrency in detail, it is helpful to place this specialized asset into proper context. The overarching category under discussion is called *digital currency*. Digital currency refers to all monetary assets in digital form whether the money it represents is actually a nation's currency (e.g., dollars, euros, or yen) or whether it is privately issued. *Virtual currency* is not connected to a nation's actual currency, and is instead "an electronic representation of monetary value that may be issued, managed and controlled by private issuers, developers, or the founding organization." Jake Frankenfield, *Virtual Currency*, INVESTOPEDIA (Aug. 17, 2019) https://www.investopedia.com/terms/v /virtual-currency.asp. In other words, you cannot hold virtual currency in your hand like you can with hard currency. Virtual currency is nothing more than ones and zeros stored on computer media. Virtual currency is not connected to a nation's actual currency but is instead "issued, managed and controlled by private issuers, developers, or the founding organization." *Id*. *Cryptocurrency* is virtual currency which uses sophisticated cryptography to make certain that transactions are secure and authentic. *Id.*

The discussion below is admittedly simple and omits sophisticated high-level computer discussion. Nonetheless, the discussion should provide the estate planner with a basic understanding of the workings of cryptocurrency.

A cryptocurrency is "born" through a computer process called *mining*. The "parent" of the virtual currency creates complex mathematical equations which the parent expects other people (the *miners*) to solve using high-powered computers. As a reward for solving these equations, the miners receive a virtual coin which they may then use to purchase real-world assets assuming they can find someone willing to accept it. As more coins are mined, it becomes harder (that is, more processing power is needed over a longer period of time) to mine each subsequent coin until a cap is reached either because one was provided by the parent or mining is no longer a cost-effective way of obtaining a coin.

These virtual coins rely on *blockchain* technology for security and validity. A blockchain is a distributed database often referred to as the *ledger*, that is, a list of transactions and their details such as the number of coins added or subtracted along with the date and time of the transaction, which is held by individuals who agree to share the database with all other users of the same database of virtual currency. The database is then continuously updated and synchronized. This results in all users having the complete record of the virtual currency instead of having only one central computer or entity that processes all transactions. Each transaction or *block* is added to the chain along with a timestamp and link to the

previous block. These transactions immediately revise all of the other copies of the database.

The owner of cryptocurrency has a very long and complex "password" called a *private key* to access the portion of the blockchain containing the owner's coins. This private key is mandatory to access the owner's virtual currency. To transfer virtual currency from one person to another person as payment for goods or services (or perhaps as a gift), the owner uses the owner's private key to authorize the transaction and then sends a message to the recipient containing a *public key* which is mathematically related to the location of the owner's virtual currency so that the recipient can receive the transfer. Complex software running on many different computers then verify the transaction. If the transaction is determined to be valid by enough computers, it becomes the next block in the chain. "To prevent people from generating counterfeit currency, the math required to verify a transaction takes so much computing power that no one user or group could do it." Alexander George, *Did You Miss the Cryptocurrency Boat?*, POPULAR MECHANICS, Apr. 2018, at 16, 17. In fact, one writer claims it would take the world's most powerful supercomputer over a trillion years to determine the owner's private key from the public key. *See* Prypto, *Bitcoin Public and Private Keys—Dummies*.

There are two primary ways that various cryptocurrency networks go about verifying the transactions that occur on their blockchains. The first way, which is deemed more secure but less efficient, is done in a process referred to as "proof of work." This is the scenario where a miner receives a reward for verifying transactions on the ledger. More than one miner will verify the same transaction, and often a transaction will be verified several times. This system ensures the open-access security of the blockchain, but can be costly in terms of computing power. The other type of verification process is known as "proof of stake." This system attempts to conserve resources by using a preference-based model to choose who will verify the next transaction based on the amount of that user's ownership, or 'stake,' in the cryptocurrency. See Sean Williams, *Cryptocurrencies Explained, in Plain English*, THE MOTLEY FOOL (Jan. 22, 2018) https://www.fool.com/investing/2018/01/02/cryptocurrencies-explained-in-plain-english.aspx.

Most cryptocurrency owners do not need to concern themselves with these details. Businesses called *cryptocurrency exchanges* have sprung up which handle the complex details making it easy for a person to buy, sell, and transfer their virtual coins such as Coinbase and Uphold. *See* Finder, *Cryptocurrency Exchange Finder* (Sept. 13, 2018), (indicating that over 200 cryptocurrency exchanges exist). For example, these exchanges hold the private keys and public keys and generate the messages necessary to effectuate transfers.

Cryptocurrency resides in "wallets" that can be stored in many different ways such as on an exchange accessed over the Internet, software on a computer, tablet, or cell phone, or on a dedicated flash drive. To be able to retrieve cryptocurrency and transfer it, you must have the private key or the *seed phrase*, that is, a list of random words which allows the person to recover the wallet containing the virtual currency. A seed phrase would look something like this "warlock implode lawyer drink love close cactus river street double water most." These words are tied to the private key through a complex computation process. The seed phrase needs to be kept secure at all times. Otherwise, anyone with knowledge of the phrase could access the currency. See *Seed Phrase* Bitcoin Wiki. If the wallet resides on a commercial exchange, the cryptocurrency may be accessible by a person who knows the user name, password, answers to security questions, and has the ability to satisfy other verification steps.

B. Benefits of Cryptocurrency

1. Security

Because of the high-level of encryption, cryptocurrency is extremely safe from being used by an unauthorized person unless the owner is careless in protecting the owner's private key or seed phrase. In addition, because the ledger is

stored on many computers all over the world, it is very safe against hacking and other cyber attacks.

However, this security is necessarily reliant upon the integrity of the exchange upon which the cryptocurrency is being used. If the exchange is compromised, then the security of the private key is also compromised. This particular type of security breach is what leads to many of the hackings that critics of cryptocurrency point to when discussing its relative insecurity in terms of actually ensuring ownership of one's cryptocurrency. It is important for those handling estates with cryptocurrency assets to understand the distinction between the security that is gained from the blockchain verification technology itself, as compared to the security of the exchange.

Even further, it is important to remain cognizant that real humans and not computers are the ones who will make the decisions in terms of how various blockchains will be regulated and how big questions regarding network security will be approached. For instance, after an exploitation of code during a round of capital-raising for Ethereum, a large amount of ether (the primary trading unit) was "siphoned" from the capital fund. Instead of treating the ether as stolen and simply moving forward, the creator of the platform, via a software update, basically reset the entire system to the point on the chain prior to the exploitation. While the move created what is known as a "fork" in the cryptocurrency and dissatisfied some holders, it also led to a philosophical discussion about the intervention. Most importantly for the purposes of the estate planner, this example highlights the limits of the security provided by these assets. See Jonathan Ore, *How a $64M Hack Changed the Fate of Ethereum, Bitcoin's Closest Competitor*, CANADIAN BROADCASTING CORPORATION, (Aug. 28, 2016) https://www.cbc.ca/news/technology/ethereum-hack-blockchain-fork-bitcoin-1.3719009.

2. Privacy

Cryptocurrency is virtually untraceable and sometimes gets a "bad rap" as being used by people involved in illegal activities such as drugs, gun-running, murder for hire, and prostitution. Of course, the same could be said of traditional hold-in-your-hand cash which is also normally untraceable absent the recording of serial numbers, being marked with invisible ink, or containing traceable electronic devices.

Many individuals do not wish for their financial transactions to be public for reasons that do not involve covering up unseemly activities. Instead, they believe that it is no one's business how much they own, what they buy, and what they sell. Perhaps they merely want to avoid the endless advertisements that appear after making a purchase on a traditional website which collects a considerable amount of private data.

However, those who interact with testators or other clients who wish to preserve their privacy through the use of cryptocurrency in their estate planning should be cautioned that while the blockchain itself is close to anonymous, exchanges themselves can be forced to divulge information about their users. Less than two years ago, the Internal Revenue Service (IRS) won a court case against a popular cryptocurrency exchange, mandating that the exchange divulge information on almost 15,000 users who, over the period of 2013-2015, engaged in individual transactions valued at over $20,000 at the time of the exchange. *United States v. Coinbase, Inc.*, No. 17-cv-01431-JSC, 2017 U.S. Dist. LEXIS 196306 (N.D. Cal. Nov. 28, 2017). While in this action the court did eventually limit the initial scope of the government's information request, the larger takeaway for estate planners is that transactions over cryptocurrency exchanges are not as anonymous as popularly perceived. Further, during the litigation the IRS revealed that less than one thousand taxpayers reported cryptocurrency gain or loss in 2014 and 2015, so stepped-up enforcement is expected to continue. Jeff John Roberts, *Only 802 Told the IRS About Bitcoin*, FORTUNE (Mar. 9, 2017), https://fortune.com/2017/03/19/irs-bitcoin-lawsuit.

3. Shorter Transfer Delay, Lower Cost, and Finality of Transfer

Transferring hard currencies takes time (often many days or up to a week or more), involves many intermediary steps (e.g., customer, customer's bank, intermediary banks, business's bank, and business), and incurs transfer fees. On the other hand, transfers of cryptocurrencies may occur immediately or within a few minutes and, unless an exchange is used, without a transfer cost. Even if an exchange is involved, the cost is often considerably less than traditional banking fees.

An additional advantage is the finality of the transfer that cryptocurrency's peer to peer blockchain technology provides. With other electronic transactions which are denominated in government currency, there are significant periods of time spent waiting for the transaction to close, and any number of actors that could stop, reverse, or undo the transaction. On the blockchain, once a transaction has been verified and added to the blockchain, there is no practical way to go about reversing the transaction.

C. Risks of Cryptocurrency

1. No Recovery Without Private Key or Seed Phrase

If the owner of cryptocurrency forgets, misplaces, or loses the private key and seed phrase, there is no way the owner can recover it. There is no "forgot password" link that the owner can use to recover the private key or seed phrase. If the cryptocurrency is stored on an exchange, there will be a greater chance of being able to regain a lost password because the owner is gaining access to the exchange rather than the cryptocurrency directly.

James Howells of Newport, Wales learned this lesson the hard way. He chose to store his 7,500 Bitcoins on a hard drive in 2009 when they were nearly worthless. Several years later, he discarded the hard drive in the trash which ended up in a landfill the size of a football field. He searched the landfill to no avail even after funding a more extensive search with an Indiegogo account. *See* Stephen Shankland, *UK Man Tries to Retrieve $7.5 Million in Bitcoins from Dump*, CNET, Nov. 29, 2013. If he had those Bitcoins on October 6, 2025 when Bitcoin peaked at over $126,000, they would have been worth approximately $947 million.

Another example touches upon a likely estate planning scenario that highlights the important distinction between the security of the cryptocurrency's blockchain itself and the security of an exchange. Early in 2019, a thirty-year-old owner of a cryptocurrency exchange died unexpectedly while on an aid mission to India, and "a sworn affidavit [by his wife] as she filed for credit protection… [stated he] held 'sole responsibility for handling the funds and coins.'" James Rogers, *$190 Million Gone Forever? Crypto Boss Dies with Passwords Needed to Unlock Customer Accounts*, FOX NEWS, (Feb. 4, 2019) https://www.foxnews.com/tech/cryptocurrency-exchange-chief-dies-with-passwords-needed-to-unlock-customers-190m-reports-say. The owner's digital key was necessary to access the cryptocurrency assets held in what the company called "cold wallets" but that digital key was held on the decedent's laptop. In filing for creditor protection, the company publicly acknowledged its efforts to locate the key and free the assets had been unsuccessful. This unfortunate scenario could have been avoided with proper estate planning, but serves to highlight the drawbacks of the peer-to-peer privacy model.

2. Value Fluctuation

Cryptocurrency is not backed by any government and thus its value is subject to tremendous fluctuation. Even the most popular virtual currency, Bitcoin, has seen huge value shifts. For example, in 2010, one Bitcoin was worth $.01 and had increased to $1,000 by January 1, 2017. At the end of 2017, one Bitcoin was worth almost $20,000. On October 6, 2025, the value of one Bitcoin was over $126,000 with the value changing by several dollars every second.

Some in the cryptocurrency industry have recognized the need for greater stability in order to meet investors' desires, and have created

"stablecoins" to enjoy the privacy and security benefits of cryptocurrency while minimizing the negative effects of holding or trading in what has historically been a volatile, unstable market. To alleviate the rapid swings, some of these cryptocurrencies are physically pegged to a particular currency, like the U.S. dollar, or to a certain commodity, like gold. Other stablecoins "achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives." Adam Hayes, *Stablecoin*, INVESTOPEDIA (Sept. 1, 2019) https://www.investopedia.com/terms/s/stablecoin.asp. In fact, the capital fund being raised by Ethereum during their large cryptocurrency heist in 2016 was designed to be pegged against the U.S. dollar, and allow for up to 50% swings in valuation of the underlying cryptocurrency asset before investors lost actual invested capital as denominated in U.S. dollars.

3. No Regulation

Cryptocurrencies are not subject to any central authority, such as a government or governmental entity, which can provide a type of security or insurance from the value fluctuations discussed above, cheaters, scammers, and other evil conduct. If something "happens" to cryptocurrency, the owner is out-of-luck without any recourse. For example, "[in] February 2014, the then-largest bitcoin exchange, Mt. Gox, went bankrupt after hackers stole some 850,000 bitcoins that at the time were worth roughly $450 million." Rebecca Patterson, *The Hype and Hope of Bitcoin and Blockchain*, Bessemer Trust, Second Quarter 2018, at 1, 3. However, defenders of cryptocurrency correctly point out that the compromise of an exchange (or wallet) is not a threat to the actual security of the blockchain's encryption, and liken the situation to a bank robbery – poor security at a bank does not inherently threaten the security of the monetary system itself. Saifedean Ammous, *Can Cryptocurrencies Fulfill the Functions of Money?* 10 (Columbia University Center on Capitalism and Society Working Paper No. 92, Aug. 2016). https://capitalism.columbia.edu/files/ccs/working_page/2017/ammous_cryptocurrencies_and_the_functions_of_money.pdf ("For somebody to 'hack' into the Bitcoin network and change the issuance schedule, they would be required to marshal processing power larger than 17,000 times the power of the world's top 500 supercomputers."). It also appears that while cryptocurrencies are not under the direct control of any government authority, not all coins are operationally the same in terms of a purely decentralized approach to their blockchain source code – thus manipulations of the asset can take place, albeit in limited form. However, as demonstrated by the unfortunate passing of the Canadian exchange owner, there is no entity like the Federal Deposit Insurance Corporation or similar government body to "maintain stability and public confidence" through insuring the unlucky cryptocurrency investor, nor a Federal Reserve Bank tasked with a mandate and power to "moderate…the U.S. economy" through currency stabilization efforts. While some individuals with cryptocurrency assets may believe the lack of regulation surrounding their investment to be a net positive, it is important for estate planners to acknowledge the inherent risks that come with a currency largely free of government regulation by design.

D. Prudent Investment and Fiduciary Concerns

Cryptocurrency is risky. As one commentator stated, it is more risky than gambling. "In roulette, if you put $1 on every number, you'll spend $38 and be guaranteed to get exactly $36 in return. You could buy $1 of every cryptocurrency and they might all end up worthless." Alexander George, *Did You Miss the Cryptocurrency Boat?*, POPULAR MECHANICS, April 2018, at 16, 17.

Under the prior prudent person rule, a trustee could not invest in cryptocurrency absent express permission in the trust because of this risk. However, under the Uniform Prudent Investor Act effective in most states, trustees must make investment decisions "in the context of the trust portfolio as a whole and as part of an overall investment strategy having *risk* and return objectives reasonably suited to the trust." Accordingly, the trustee needs to determine with

respect to each trust, after considering all of the circumstances whether investment in cryptocurrency is allowed or perhaps even required. The author's anecdotal conversations with corporate trustees reveal a tremendous hesitancy to invest in cryptocurrency without express permission in the trust instrument from the settlor, a release by the beneficiaries, or authorization in a court order. *See also* Suzanne Walsh, *Every Day is Bitcoin Pizza Day: What Clients and Estate Planners Need to Know about Cryptocurrency*, Lexology.com, Sept. 6, 2017.

E. Taxation and Classification of Cryptocurrency

Digital currencies have value, and so legally they must be reported in the valuation of an estate. In 2014, the IRS indicated that cryptocurrency is "property" rather than currency. IRS Notice 2014-21. Accordingly, cryptocurrency is subject to capital gains tax rules. The fair market value of cryptocurrency is to be calculated "by converting the virtual currency into U.S. dollars . . . at the exchange rate, in a reasonable manner that is consistently applied." *Id*. There are sources that keep historical records of the value of a cryptocurrency as of a certain date, such as Poloniex and Coinmarketcap.com. *See* Michael Goldberg, *Estate Planning for Cryptocurrency*, 106 ILL. B.J. 38 (2018). These resources enable users to access cryptocurrency records much like they can access historical records of stock. A fiduciary should be aware of these basis rules, as there are situations where it could be more advantageous to purchase with cash or with cryptocurrency depending on its impact on the taxpayer's basis. See Sasha A. Klein & Andrew R. Comiter, *Bitcoin: Are You ready for This Change for a Dollar?*, Prob. & Prop. March/April 2015, at 11, 13.

Further, there is the potential for scenarios beneficial to the decedent's beneficiaries to arise due to of this distinction. Because the property is not treated like a fiat currency, "certain planning techniques can maximize the 'step-up' in tax basis that occurs at death for certain assets. This planning may later reduce the inheriting owner's tax burden significantly if, for example, the inheriting owner were to sell assets after the death of the original owner." Geoffrey S. Kunkler, *Preparing for the New Frontier in Trusts & Estates: Blockchain and Cryptocurrency, Incorporating Cryptocurrencies into Estate Planning*, 29 OHIO PROB. L.J. 5 (2018). The basis of a bitcoin for a person acquiring it from a deceased owner will be the fair market value as of the date of the owner's death. IRC § 1014(a)(1) (2018).

Taxpayers who are engaged in the mining of cryptocurrency must compute their taxable gross income based on the fair market value of the cryptocurrency on the date received. The initial metaphysical quandary of taxing digital mathematical creations is explained by characterizing mining as the reception of existing virtual currency in exchange for computer services. Other employment tax issues include the assessment of the self-employment tax against miners of cryptocurrency, and the withholding and reporting requirements of wages paid by an employer in the form of cryptocurrency under Federal Insurance Contributions Act (FICA) and Federal Unemployment Tax Act (FUTA). IRC § 1401 et seq. (2018).

A significant issue left unaddressed by the Notice 2014-21 is whether the property classification applied to cryptocurrency falls under the tangible or intangible property distinction. Some commentators have recognized that the Notice's treatment of miners' realized income from mining activity inherently rejects a tangible personal property approach. Sasha A. Klein & Andrew R. Comiter, *Bitcoin: Are You Ready for This Change for a Dollar?* PROB. & PROP., Mar./Apr. 2015, at 11, 13. Another commentator has acknowledged that cryptocurrency does have characteristics making it amenable to a tangible personal property characterization. Max I. Raskin, *Realm of the Coin: Bitcoin and Civil Procedure*, 20 FORDHAM J. OF CORP. & FIN. L. 969 (2015). These distinctions are important, particularly in the context of charitable deductibility and transfer by a noncitizen nonresident if the situs of the cryptocurrency is in the United States. While multiple professional interest groups such as the

American Institute of Certified Public Accountants (AICPA) and the American Bar Association's Tax Section have approached the IRS with requests for additional guidance, only guidance on the relatively narrow treatment of 'hard fork' and 'airdrop' occurrences has been issued as of late 2019. I.R.S. News Release IR-2019-167 (Oct. 9, 2019). The IRS describes a hard fork as "when a distributed ledger undergoes…a permanent diversion from the legacy or existing distributed ledger." Rev. Rul. 2019-24, 2019 I.R.B. LEXIS 384, 1 at 2. It further suggests that an airdrop, or distribution of new cryptocurrency units to existing holders at the time of the fork, often follows the hard fork event, though it does not need to. However, as the interest group letters make clear, there are still many issues to resolve regarding the taxation of cryptocurrency.

Additional considerations apply for states which feature an income tax and, if the cryptocurrency is considered tangible, sales taxes imposed on the sale of tangible personal property within the taxing state. For internet sales tax purposes, "the location of a cryptocurrency wallet within a state may be a sufficient nexus for that state to tax sales of cryptocurrency" that occur for a particular wallet. Austin Bramwell, Abigail Rosen Earthman, Benetta P. Jenson & Suzanne Brown Walsh, *New Kids on the Block(chain): Planning with Bitcoin and Cryptocurrency*, 53 HECKERLING INST. ON EST. PLAN. 14 (2019).

The question of whether cryptocurrency can be classified as a "security" such to come under the jurisdiction of the Securities and Exchange Commission (SEC) is increasingly being answered in the affirmative. In a June 2018 speech, SEC Director of Corporate Finance William Hinman expressed that while Bitcoin and Ether specifically were not securities "if there is a centralized third party, along with purchases with an expectation of a return, then it is likely a security." *Id.* at 42. Additionally, enforcement actions have proceeded along similar lines, applying the *Howey* test for a general determination of a security in an admittedly "highly fact-specific" inquiry. *Id.* at 43. It is more clear that cryptocurrency may be classified as a "commodity" for the purposes of the Commodity Exchange Act (CEA) and be subject to the jurisdiction of the Commodity Future Trading Commission. *Id.* at 45. Citing the definition of commodity in the CEA, the CFTC noted it encompassed a broad inclusion of "among other things, 'all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in.'" *Id.* Estate planners should seek advice from qualified professionals if these complicated scenarios should arise in their practice.

F. Recommendations

As time marches by, an increasing number of your clients will own cryptocurrency. Only with proper planning, however, will the value of this property be available to the client's successors in interest. Here is a summary of the key steps an estate planner should take.

- Early in the estate planning process via client intake forms, questionnaires, or interview questions, ascertain whether your client owns (or plans to acquire) cryptocurrency.
- A cryptocurrency owning client needs to keep detailed records of the date of each virtual currency purchase and the amount so that capital gains income tax planning can be effectively accomplished such as (1) selling and paying the tax (or taking a loss) now, (2) gifting with a carry over basis, or (3) allowing it to pass at death to give the beneficiary a stepped up basis.
- If the client owns cryptocurrency stored in a software wallet not connected to an exchange, it is essential to make arrangements to protect and then transfer the private key or seed phrase to the person whom the client wishes to own the virtual currency after the client's death. Storing the key or phrase in a safe deposit box is a frequently used technique.
- If the client owns cryptocurrency stored on an exchange, then protection, storage, and transfer of the user name, password, and

security question information is needed. In addition, some exchanges use two-factor authentication. For example, after entering the user name and password on the exchange's website log-in page, the exchange sends a numerical code to the owner's cell phone which the user must then enter to access the owner's account. If this is the case, the cell phone itself and how to access it must also be protected. *See* Michael J. Kearney & Joseph B. Doll, *Considerations in Estate Planning for Bitcoin, Ethereum, and Other Crypto-Currencies*, www.estaxtrustsestatesblog.com (Apr. 26, 2018).

- If the client owns cryptocurrency stored on a hardware wallet (flash drive), arrangements to reveal to the intended beneficiary both the drive's location and the keys, phrases, or codes needed to access it must be made. As with software wallets, keeping the device and phrase in a safe deposit box is often an effective protection method.
- The estate planner needs to ascertain whether the client wishes to make a specific gift of any cryptocurrency upon death (either to a person or to a trust) or whether it is merely to become part of the decedent's general estate. If a specific gift is intended, the gift provision needs to be carefully drafted to transfer the cryptocurrency but *not* contain the private key, seed phrase, passwords, or other access information. Instead, the will should describe how the beneficiary (or trustee, if the transfer is to a trust) may obtain this information such as on a flash drive in a safe deposit box or from a trusted individual.
- After a person has died, search diligently for the existence of digital currency. If the decedent used an exchange to purchase the cryptocurrency, the exchange account will typically be linked to a bank account or credit card, so the decedent's bank records or emails may provide a clue that the account exists. Signs of cryptocurrency can also be spotted on the decedent's phone, tablet, or computer if a mobile wallet or offline wallet was used. Another, albeit much rarer sign, would be a room filled with high-end computers which could indicate the decedent was a miner.
- If cryptocurrency is located, the executor or administrator will need to deal with it appropriately. The property is just like any other estate asset. It needs to be preserved as much as possible if it is subject to a specific bequest in the decedent's will. If it is not, the personal representative will need to decide whether to retain the cryptocurrency or liquidate it for United States currency. As discussed above, this will require the executor or administrator to act as a reasonably prudent investor.
- For inventory and transfer tax purposes, the value of the cryptocurrency is the fair market value at the date of death. Several websites maintain historical exchange rate records such as Poloniex, Bittrex, and Coinmarketcap. *See* Michael Alan Goldberg, *Estate Planning for Cryptocurrency*, ILL. B.J., Feb. 2018, at 38, 49.

IX. NON-FUNGIBLE TOKENS

Your client may own non-fungible tokens (NFTs) and ask you for estate planning advice. Would you be caught off-guard and give your client the classic "deer in the headlights" look? Obviously, that would not be prudent. To make sure this doesn't happen to you, this section uses a FAQ approach to provide you with the background and information you need so that you will understand NFTs and how to give your client sage advice on how to handle them during the client's lifetime and upon death.

A. What is a non-fungible token?

A non-fungible token (NFT) is an electronic asset that is uniquely identified. It is non-fungible meaning that each NFT is distinguishable from all

other NFTs; no two are the same like snowflakes. It is a digital token rather than a physical token like a casino chip or a coupon. By comparison, cryptocurrency like Bitcoins are fungible tokens in that every Bitcoin is the same as every other Bitcoin.

B. What do NFTs represent?

NFTs may represent photographs, videos, music, artwork, on-line gaming content, tweets, and other types of digital files. They are electronic representations (tokens) of this property compared to a physical token like a casino chip that represents a specific number of physical dollars.

Unless specifically included, the NFT does not encompass the underlying intellectual property such as the copyright for the work the NFT represents.

C. Where are NFTs stored?

NFTs are stored on a *blockchain* that certifies that the digital asset is unique and not interchangeable with another asset. A blockchain is a distributed database often referred to as the *ledger*, that is, a list of transactions and their details such as the date and time of the transaction, which is held by individuals who agree to share the database with all other users of the same database. The database is then continuously updated and synchronized. This results in all users having the complete record of the NFT transactions instead of having only one central computer or entity that processes all transactions. Each transaction or *block* is added to the chain along with a timestamp and link to the previous block. These transactions immediately revise all of the other copies of the database. This results in a record that is virtually impossible to hack.

D. How does a person create an NFT?

The creation process of an NFT is called "minting." NFTs are minted on a blockchain in a similar manner to cryptocurrency. Currently, Ethereum is the most popular platform but other platforms may also be used. The creator such as an artist, performer, or author links the NFT to the specific item of digital property that it represents. To enhance the value of an NFT, the creator may promise to limit the number of NFTs created. For example, the creator may decide to make only one NFT that represents the digital property or limit creation to a specified limited number (e.g., a series of ten so purchasers would own 1 of 10, 2 of 10, etc.). The minting process is described in more detail in a later FAQ.

E. Why does a person create an NFT?

A person creates an NFT in the hopes of selling the NFT to make a profit. Each NFT is unique; no two NFTs are the same. They may not be copied. The name of an owner of an NFT is part of the public blockchain record and thus anyone can verify ownership. NFT creators may sell their work on a global market as well as retain the right to receive royalties each time the NFT is sold by using smart contract technology.

F. I still am confused. Are there old-school analogies that may help me understand NFTs?

Yes. NFTs are digital counterparts of physical autographs, baseball cards, stamps, coins, comic books, artworks, and other similar collectible items.

G. What is the value of an NFT?

The value of an NFT depends on market forces (supply and demand) because the NFT has no intrinsic value just like other collectible items. For example, one baseball card may have significant value because it is scarce and highly sought after by collectors while another card has little or no value because a huge number of the cards are available or the person depicted is not famous.

H. What are some examples of notable NFTs?

- The NFT of Beeple's (Mike Winkelmann) *Everydays: The First 5000 Days*, a collage of 5,000 individual pieces created over a 13-year period, sold for $69,346,250 by Christie's on March 11, 2021. This is said to be the most expensive NFT ever sold and the first by a major auction house. See Jacob Kastrenakes, *Beeple Sold an NFT for*

$69 Million, The Verge (Mar. 11, 2021).

- In the on-line game CryptoKitties, a digital cat sold for $172,000. The game is designed for players to buy, trade, and breed the digital cats. However, the cost is rarely this high. In 2018, the average price paid for a CryptoKitty was $60 with the median price being $9. See Mark Serrels, *Someone Just Bought a Cryptocurrency Cat for $172,000*, CNet (Sept. 4, 2018).

- An NFT entitled *Lebron James: Dunk From the Top* sold for $208,000. See Elizabeth Lopatto, *Top Shot is Playing the Long Game in the NFT Craze*, The Verge (Mar. 30, 2021).

- Major League Baseball sold a digital copy of Lou Gehrig's *Luckiest Man* speech for $70,400 on July 4, 2021. See Kenneth Rapoza, *MLB Goes All In On NFTs With Lou Gehrig, Now LA Dodgers Art. Why is This Still a Thing?*, Forbes (July 12, 2021).

- The swag bag at the recent Oscars included an NFT of Chadwick Boseman, the actor who portrayed the Marvel superhero Black Panther. See Nancy Dillon, *Chadwick Boseman Gets NFT Tribute in Oscar Nominee Swag Bags*, NY Daily News (Apr. 25, 2021).

- An NFT of the first tweet by Jack Dorsey, the co-founder of Twitter, sold for $2.9 million. See Taylor Locke, *Jack Dorsey Sells His First Tweet Ever as an NFT for Over $2.9 Million*, CNBC (Mar. 22, 2021) (The tweet says, "just setting up my twttr," and was posted on March 21, 2006).

I. Other than collectibles, what are some other possible uses of NFTs?

NFTs could be used to secure and authenticate physical assets, both personal and real property. For example, Nike has patented a system for using NFTs to protect against counterfeit shoes so subsequent purchasers of high-end sneakers would be certain of their shoes' authenticity. See Hilary George-Parkin, *How Nike's Likely NFT Move Could Shake Up the Sneaker Resale Market*, Footwearnews.com (Apr. 16, 2021).

There is also speculation that NFTs could operate as a highly secure method of transferring title to real property and to store electronic wills and other estate planning documents.

J. How do NFT owners store and access their NFTs?

NFTs reside in digital "wallets" that can be stored in many different ways such as on an exchange accessed over the Internet, software on a computer, tablet, or cell phone, or on a dedicated flash drive. To be able to retrieve an NFT and transfer it, the person must have the private key or the *seed phrase*, that is, a list of random words (typically 12, 18 or 24 words) which allows the person to recover the wallet containing the NFT. A seed phrase would look something like this "warlock implode lawyer drink love close cactus river street double water most." These words are tied to the private key through a complex computation process. The seed phrase needs to be kept secure at all times. Otherwise, anyone with knowledge of the phrase could access the NFT. If the wallet resides on a commercial platform, the NFT may be accessible by a person who knows the user name, password, answers to security questions, and has the ability to satisfy other verification steps.

K. What is the first step I need to take regarding NFTs when working with an estate planning client?

It is essential for you to determine if your client owns or intends to purchase NFTs. You should include a question on your client intake questionnaire or in your initial client interview. If you do not know your client owns NFTs, you will not be able to help your client plan for them properly.

L. What type of records should a client keep about NFTs?

The client must keep careful records of the price paid for each NFT and the price for which it is sold so that the correct amount of capital gain or loss is reported for tax purposes.

M. Is there a special concern if the client purchases an NFT with cryptocurrency?

Yes. Many clients will purchase NFTs with cryptocurrency rather than traditional money which will lead to an additional concern. Cryptocurrency is property, not money. See I.R.S. Notice 2014-21. Thus, if a client uses cryptocurrency to purchase an NFT, a capital gain or loss will occur based on the price the client paid for the cryptocurrency that the client used to purchase the NFT. This gain or loss must be reported for tax purposes.

N. Should the client consider holding NFTs in a business entity?

Yes. The client may wish to hold the NFT in an entity such as a limited liability company (LLC). Potential advantages include (1) the ease of transfer of LLC interests compared to transferring the NFT itself which requires a blockchain transaction, (2) transfer tax discounts may be possible as the LLC interests may be minority in nature or there may be a lack of marketability, and (3) asset protection. See Joshua Caswell & Leigh E. Furtado, *NFTs for Estate Planners, Not Just a Token Concern*, PROB. & PROP., Sept./Oct. 2021, at 10, 13.

O. How should the client protect the information needed to access NFTs?

The private key or seed phrase required to access the digital wallet in which the NFT is stored must be protected while the client is alive and then transferred to the beneficiary upon the client's death. Just like cryptocurrency, without the means of accessing the NFT, it will be lost forever. Some clients elect to keep this information in their safe deposit boxes in old-school written form or on a flash drive or other digital media which may also be encrypted to add another layer of protection. Others will engrave the information on a metal plate to assure it will survive fires, floods, hurricanes, tornadoes, earthquakes, and other disasters. Some people will use complex methods such as dividing the seed phrase into sections and storing them in different places so that only by bringing them all together like the Infinity Stones can the NFT be accessed. An even more sophisticated method is Shamir Secret Sharing where an algorithm is used to divide the seed phrase into multiple seeds (e.g., five) and the client indicates how many (e.g., 3) need to come together to create the entire seed phrase. See Sidd, *The Ultimate Guide to Safe Seed Phrase Storage*, http://whatismoney.info (last visited Nov. 14, 2021).

P. How should a client's will address NFTs?

The client may make a specific gift of individual NFTs or a general gift of all NFTs the client owns. If NFTs are not specifically mentioned, they will pass under the will's residuary clause. As discussed previously, it is important to provide a method of transferring the NFT access information to the beneficiary outside of the will. Access information should not be included in the will because it becomes a public document once filed for probate.

If the client's NFT collection is extensive, the client may wish to consider appointing a separate "digital executor" who has the responsibility of dealing with digital assets for the benefit of the client's estate. Even if a separate person is not appointed, the client may wish to direct the executor to hire a person with the skills needed to prudently manage NFTs.

Q. I am a personal representative of a decedent's estate. Can I access the decedent's NFTs?

Yes, a personal representative has the authority to access NFTs under the Revised Uniform Fiduciary Access to Digital Assets Act which has been enacted in almost all states. However, the authority to access NFTs is worthless unless the personal representative has the access information.

R. I am a personal representative of a decedent's estate. Is there anything special regarding NFTs about which I should be immediately concerned?

Yes, you should document the value of the NFT as of the date of the decedent's death. The beneficiaries who receive NFTs are entitled to a step-up in basis to the value of NFT as of the date of the decedent's death rather than the decedent's basis. I.R.C. § 1014. If the NFT has increased in value since the time of purchase, being able to document the date of death value will reduce the amount of capital gains taxes owed when the beneficiary sells the NFT.

S. I am a trustee. Can I retain NFTs in a trust or invest in NFTs?

In almost all states, a trustee is bound by the prudent investor standard, that is, investment decisions must be made "in the context of the trust portfolio as a whole and as part of an overall investment strategy having risk and return objectives reasonably suited to the trust." The value of NFTs is extremely volatile and would likely be considered too risky of an investment for a prudent investor. Accordingly, a trustee should be very hesitant to retain or invest in NFTs without express permission from the settlor in the trust instrument, a written release by all beneficiaries, or authorization in a valid court order.

T. Are there any religious-based considerations I need to keep in mind with respect to NFTs?

Yes. Some religions may frown upon its members investing in cryptocurrency and perhaps NFTs as well. For example, at least one Islamic council ruled that using Bitcoin and other cryptocurrencies as a means of payment is unlawful under Islamic law because they are deemed gambling due to the price volatility. See *Indonesian Islamic body forbids crypto as currency*, CNN.Com (Nov. 11, 2021).

U. If I plan on advising clients about NFTs, is there anything else you would recommend that I do?

Yes, I recommend that you create a digital wallet and create an NFT. You will learn a great deal by going through the process yourself and then you will not be like a marriage counselor who has never been married giving advice on how to maintain a successful marriage. Here are the basic steps you can take:

- Locate a website or application that streamlines the NFT minting process considering the ease of use and the cost (referred to as gas) you will pay to compensate for the computing energy needed to process and validate the NFT transaction. (I used https://www.Mintable.app.) Create an account with a user name and password. Note that most apps link to the most popular NFT blockchain, Ethereum. Many of these platforms will walk you through the process described below in a step-by-step manner.

- If you do not already have a digital wallet in which you can store NFTs, create one and obtain the seed phrase. (I used https://MetaMask.io which you can access on your computer or via a phone app.)

- Link the app to the digital wallet using an extension to your Internet browser or smartphone app.

- Take and save a picture on your computer or phone of something you think is interesting, e.g., your office, favorite pet, a selfie, the view out your window, etc.

- Follow the steps in the app to upload the picture and mint an NFT linked to the picture.

- You can either keep the NFT in your wallet, transfer it to someone else's wallet, or list it for sale at a fixed price or as an auction item.

V. If my client mints NFTs, are there any additional special warnings I should provide the client?

Yes, the client needs to be leery of creating NFTs that link to copyrighted work without permission of the copyright holder. "[U]nder U.S. copyright law, the creator retains exclusive rights to reproduce and distribute copies of, make derivatives of, and publicly perform and display the copyrighted work." Richard Acello, *Big Money*, ABA J., Oct./Nov. 2021, at 25, 26. Thus, a client should not mint an NFT that is linked to copyrighted property such as songs, videos, and artwork.

W. Why should a charitable organization consider accepting NFT and crypto-currency donations?

NFT investors are disproportionately charitable, and the recent significant appreciation of NFTs may lead many investors to consider donations as a potential method of tax alleviation. One platform for crypto donations, The Giving Block, reported a total of $69 million in donations in 2021, a number that is projected to grow in the coming years. Also, organizations that operate internationally like UNICEF and the Red Cross have found accepting crypto assets to be particularly useful. Accepting crypto donations allows organizations like these to easily transfer money around the world quickly without paying wire fees.

X. Due to their volatile nature, is it risky for charitable organizations to accept crypto assets?

The valuation of crypto assets is notoriously difficult, maybe impossible, therefore it is understandable that an organization may be wary about accepting crypto donations. It may be advisable to have a policy in place that determines whether the organization will liquidate the asset immediately, which is typically recommended, or hold on to the crypto for investment. If you do choose to keep donated crypto assets, guidelines for when the organization will liquidate may also be helpful. Most platforms that assist with crypto donations will liquidate immediately, thus minimizing any risk of value fluctuations.

Y. How can a charitable organization accept crypto donations?

The first option is outsourcing the donations to a third-party platform. This may be an attractive option for organizations who wish for a "hassle-free" method for accepting crypto donations. Companies such as Bitpay, Engiven, or The Giving Block can integrate crypto donations directly to a website and convert the donated crypto into USD, with fees ranging from 1% to 5%. However, organizations with adequate capacity and expertise may seek to manage crypto donations in-house. Under this approach, an organization would need to establish an account with a crypto exchange where they would be able to accept donations directly from donors. The appeal of this approach is a lower trading cost and a wider array of tokens that are able to be accepted; however, this approach would require the organization to be more involved in the crypto donation process and more technologically savvy. Donors may also use a donor advised fund to donate crypto. In this scenario, a DAF sponsor that accepts crypto donations will generally liquidate the asset prior to it reaching your organization, making it no different than other donations.

Z. Are there any additional considerations for organizations wanting to hold on to crypto donations?

Aside from the previously mentioned volatility, another concern for organizations is regulatory risk. While lawmakers generally agree that the crypto industry needs regulation, there is little agreement concerning what that potential regulation may look like and what effect it may have on the crypto industry. Shifts in the regulatory environment could possibly devalue crypto holdings or restrict their transferability. Organizations should consider their risk tolerance when considering holding these types of assets. Aside from liquidating donated crypto assets immediately, organizations can lower risk by only accepting more established coins, such as Bitcoin or Ethereum.

AA. Are there any specific reporting requirements for crypto donations?

The IRS has made clear that charitable organizations should treat donations of crypto assets as noncash contributions. Generally, an organization can accept donations of crypto in the same manner as they accept appreciated stock or other types of property. Organizations must also file Form 8282 if they sell, exchange, or otherwise dispose of its cryptocurrency within three years after the date they originally received the property.

BB. How are crypto assets treated for accounting purposes?

The US Financial Accounting Standards Board has yet to directly address how crypto assets are to be treated for accounting purposes, despite numerous calls to do so. For some nonauthoritative guidance, the Association of International CPAs has released "Accounting for and auditing of digital assets", which may include some helpful guidance.

CC. Do crypto assets pose any ESG concerns for my organization?

A large externality associated with crypto assets is the large amount of energy that is required for their production. Bitcoin alone has an annual energy consumption that is larger than countries like Argentina and is in excess of Google, Apple, Facebook, and Microsoft combined. Further, the majority of this energy does not come from renewable sources. There are efforts in place to make crypto more efficient and consume far less energy; however, your organization should consider whether crypto donations align with your organizational mission. Another concern with crypto assets is their association with illicit activities. Given their generally pseudonymous nature, crypto is a favored medium of exchange amongst criminals and other bad actors. However, as crypto assets are gaining more widespread usage, this association is declining.

DD. Why should my client consider donating crypto assets?

Aside from the general reasons why a client might otherwise donate to charities, donating crypto can help to avoid the tax burden that the client would otherwise experience from transferring appreciated crypto into USD. Crypto investors are required to recognize any capital gain or loss that they realize upon a disposition of crypto, whether that is into USD or another cryptocurrency. A donor will not recognize gain or loss from a donation of crypto, and they also may be entitled to a charitable contribution deduction. Because of this reality, donating crypto allows more funds to reach charitable organizations than if crypto assets are first converted into USD. This also makes donations particularly enticing for crypto investors with highly appreciated assets.

EE. How can your client receive a charitable contribution deduction from a crypto donation?

If the client is itemizing taxes, the client may be able to receive a fair market value charitable deduction for the tax year in which the client made the gift. Donors seeking a deduction for their donation will need to obtain a donation receipt, which is done automatically by many platforms. If the crypto asset was held for investment for more than one year, the client may deduct the value of the gift up to 30% of the AGI for the year. If held for one year or less, the client may deduct the lesser of cost basis or fair market value at the time of the contribution up to 50% of your AGI. If the client is seeking to claim more than $500 on non-cash donations, the client will need to file Form 8283. To substantiate a deduction of over $5,000, the donor will need to obtain a qualified appraisal. This requirement is currently difficult to meet for the burgeoning crypto market, as qualified appraisers need to have two years of experience in valuing the type of property being appraised. While crypto investors hope for a relaxing of this rule in the future, crypto appraisals currently are expensive and difficult to find.

FF. What type of crypto assets can be donated?

Any crypto asset *can* be donated; however, platforms, organizations, and DAF sponsors that accept crypto will generally specify the types of cryptocurrencies and NFTs that they will accept for donations. Given the recent craze surrounding NFTs, some investors may be curious whether they are able to donate their NFTs to charitable organizations. Again, while possible, most organizations will not have infrastructure in place to accept and make use of NFTs. Instead, it is recommended that donors auction NFTs themselves and direct the payout to the charitable organization of your choice. This has become a popular option for NFT holders, and it allows for organizations to receive charitable donations in a more liquid form.

GG. What are some future issues I may be asked to address about NFTs?

There are several potential issues regarding NFTs beyond those already mentioned that may cause concern in the future. Once example is whether NFTs could be subject to federal security laws. Another example is whether NFTs are commodities so that they would be subject to regulation by the Commodity Futures Trading Commission. See Richard Acello, *Big Money*, ABA J., Oct./Nov. 2021, at 25, 26.

X. METAVERSE ASSETS

A. What is the Metaverse?

The metaverse is a network of three-dimensional virtual worlds focused on social connection. Although this sounds like a very new concept, the term was coined thirty years ago by Neal Stephenson in his novel *Snow Crash*. The book involved, among other things virtual real estate and the creation of 3-D avatars.

B. What are some early uses of the Metaverse?

For several decades, multi-player on-line video games have created virtual realities where players interact with their environments, other players, and game-specific characters. For years, players have accumulated virtual property in these games which may have significant monetary value. For example, a planet for the *Entropia Universe* sold for $6 million in 2011 and an asteroid space resort for the same game sold for $635,000 in 2010. Andrea Divirgilio, Most Expensive Virtual Real Estate Sales, Bornrich.com (Apr. 23, 2011) (also discussing other high priced sales of virtual property); Oliver Chiang, Meet The Man Who Just Made a Half Million From the Sale of Virtual Property, Forbes.com (Nov. 13, 2010). There are also reports of more "reasonable" prices for virtual items such as a virtual sword for use in *Age of Wulin* which was sold for $16,000. Katy Steinmetz, Your Digital Legacy: States Grapple with Protecting Our Data After We Die, Time Tech (Nov. 29, 2012).

C. How is the Metaverse expanding today?

Technological advances now permit users to access the metaverse via high-quality virtual reality headsets rather than a traditional gaming headset, computer, or television screen. The virtual realities are expanding from being game- or company-specific to being interactive and networked. The lofty goal is to have one place from where all virtual worlds may be accessed. In other words, instead of having compartmentalized virtual areas (e.g., walled castles), a user may travel between them all (e.g., roads). However, the standardization necessary to travel between different virtual worlds with a user's virtual assets intact is technically extremely challenging and will involved complex intellectual property issues. Thus, it is likely to be a long time before traveling between different companies' virtual worlds will be possible.

D. Other than gaming assets, what is a common type of Metaverse property?

Dozens of companies are now selling virtual versions of existing real property. For example, I purchased our home address on Tiliaverse for about $100. As with physical land, location is key. For example, the U.S. Capital's purchase price as of November 1, 2022 was $1,534.

E. How do I address Metaverse assets in a client's estate?

The first thing a prudent estate planner must do is to inquire whether their clients own metaverse assets. Only by recognizing that a client has these assets can the estate planner take the steps needed to be sure these assets are not lost upon the client's death or disability.

Metaverse assets are typically represented by NFTs and thus the same planning steps for NFTs apply such as the preservation and transfer of passwords and seed phrases. Failure to make these plans may result in a personal representative, heir, or beneficiary not having access to the asset and thus the value would be lost.

Assuming the personal representative has the access information, the representative may use the Revised Uniform Fiduciary Access to Digital Assets Act to access the virtual property and take appropriate steps to handle it in the estate. The value of the metaverse assets needs to be documented as of date of death so these assets are entitled to the step-up in basis. Unfortunately, obtaining a true market value of these assets is very difficult for lack of a standardized market.

F. How do I address Metaverse assets held in trust?

The owner of metaverse assets may transfer them to a trust. How should a trustee deal with these assets given the prudent investor standard which request investment decisions to be made "in the context of the trust portfolio as a whole and as part of an overall investment strategy having risk and return objectives reasonably suited to the trust"? The value of metaverse assets is extremely volatile. Trustees should be very hesitant to retain metaverse assets without the settlor's express permission in the trust instrument, a release signed by all trust beneficiaries, or a court approved authorization.

XI. FUTURE REFORM AREAS

A. Providers Gather User's Actual Preferences

Although most service providers have a policy on what happens to the accounts of deceased users, these policies are not prominently posted and many consumers may not be aware of them. If they are part of the standard terms of service, they may not appear on the initial screens, as users quickly click past them.

Rather than forcing these unread terms upon users, the service providers should follow the lead of Google and Facebook in developing online tools, allowing users to indicate their desires for what should happen upon the user's death. To ensure that more people make provisions, providers should offer an easy method at the time a person signs up for a new service so the person can designate the disposition of the account upon the owner's incapacity or death. For accounts already in existence, service providers should make the effort to reach out to users about their new online tool, stressing the importance of entering the required data and making it easy for them to do so.

B. Congress Amends Federal Law

Congress should amend the Stored Communications Act and the Computer Fraud and Abuse Act to make certain that fiduciary access, even if contrary to TOSAs, is not potentially subject to federal criminal sanctions. Federal law could require service providers to respect state laws on fiduciary powers, or even to ensure that all users click through an "informed consent" provision when they sign up for new services.

C. States Enact RUFADAA

As previously mentioned, as of October 18, 2026, forty-seven states, the District of Columbia, and the U.S. Virgin Islands have enacted RUFADAA. These jurisdictions acted expediently to put into place legislation that is a tremendous step in the right direction when it comes to fiduciaries' access to digital assets.

As of October 18, 2026, RUFADAA was pending in Massachusetts.

Two states that have not enacted RUFADAA and where it was not pending as of October 18, 2026:

1. *Delaware*. Delaware still has the original "enactment" of UFADAA as its current law but has not enacted RUFADAA. *See* Decedents' Estates and Fiduciary Relations, Title 12, Chapter 50 (2014).

2. *Louisiana*. Louisiana considered RUFADAA in 2016, but it was not enacted. Louisiana HB 1118 (2016). Louisiana still has its "third generation" legislation in place as summarized earlier. La. Rev. Stat. § 3191.

XII. CONCLUSION

Complications surround planning for digital assets, but all clients need to understand the ramifications of failing to do so. Estate planning attorneys need to comprehend fully that this is not a trivial consideration and that it is a developing area of law. More cases will arise regarding TOSAs, rights of beneficiaries, and the ramifications of applicable state and federal laws. The best thing clients can do at this time is to use the methods available to them to make clear their desires with regard to digital assets.

APPENDIX A – DIGITAL ESTATE INFORMATION SAMPLE FORM[1]

DIGITAL ESTATE INFORMATION FOR:

_____

I. LOCATIONS OF HARD COPY FILES AND MEDIA BACKUP

Personal records =

Financial =

Home/apartment records =

Media backups =

> The location of traditional paper records as well as where back ups of digital information are stored is very helpful.

DEFAULT INFORMATION

User names =

Passwords =

Secret questions:

Mother's maiden name =
Grade school =

> Many clients have default information which they use for many accounts. If no specific access information is provided, this at least provides a starting point.
>
> Some clients may also have a method of assigning passwords. If so, the client should provide this information.

[1] For another sample form, see James D. Lamm, *Digital Audit: Passwords & Digital Property* (2015).

Street where grew up =

ELECTRONIC DEVICE ACCESS

Device	**Website**	**Username**	**PIN**	**Password**
Computer – home				
Computer – office				
Operating System				
Voice mail – home				
Voice mail – work				
Voice mail – cell phone				
Security system				
Tablet				
e-Reader				
GPS				
Router				
DVR/TiVo				
Television				

E-MAIL ACCOUNTS

Description	E-mail address	Username	PIN	Password	Disposition Desires
Work					
Home					
School					

DOMAIN NAMES

Website/Domain Name	Webhost	Username	PIN	Password
Personal				
Business				

ON-LINE STORAGE

Name	Website	Username	PIN	Password
Dropbox				
Google Drive				
OneDrive				

FINANCIAL SOFTWARE

Item	Website	User Name	PIN	Password
Quicken				
TurboTax				

BANKING

Institution	Website	User Name	Password	ATM PIN	Security Image
Checking					
Savings					
PayPal					

STOCKS, BONDS, SECURITIES

Institution	Website	User Name	Password	Other Information

INCOME TAXES

Item	Website	User Name	PIN	Password
Federal Income tax payment	https://www.eftps.com/eftps/			
State Income tax payment				
Prior computerized tax returns				

RETIREMENT

Institution	Website	User Name	Password	Other Information

INSURANCE

Institution	Website	User Name	Password	Other Information
Health				
Life				
Property				

CREDIT CARDS

Institution	Website	User Name	Password	PIN
American Express				
Visa				

DEBTS

Institution	Website	User Name	Password	Other Information
Mortgage				
Cars				
Student Loan				

UTILITIES

Institution	Website	User Name	Password	Other Information
Electric				
Gas				
Internet				
Phone(landline)				
Phone (cell)				

Institution	Website	User Name	Password	Other Information
TV				
Trash				
Water				

BUSINESSES

Institution	Website	User Name	Password	Other Information
Amazon.com				
e-Bay.com				

SOCIAL NETWORKS

Institution	Website	User Name	Password	Disposition Desires
Facebook				
LinkedIn				
Twitter				
Instagram				

DIGITAL MEDIA ACCOUNTS

Institution	Website	User Name	Password	Other Information
Netflix				
iTunes				
YouTube				
Hulu				
Nook				
Kindle				

CYBER PROPERTY (Cryptocurrency, NFTs, Metaverse)

Institution	Website	User Name	Password	Other Information
Coinbase				
Metamask				
Decentraland				

LOYALTY PROGRAMS

Name	Website	User Name	Password
Airlines			
Grocery stores			
Appliance stores			
Starbucks			

OTHER ACCOUNTS

Name	Website	User Name	Password
Skype			
LoJack			
WoW			
HalfLife			
Flickr			
Medical records			

Name	Website	User Name	Password

APPENDIX B –SAMPLE DOCUMENT LANGUAGE

A. Wills

1. Short Form Samples

Digital Assets Other than Electronic Communications

I grant my executor full access to my digital assets other than electronic communications to the fullest extent allowed under state and federal law.

Electronic Communications

[full access to all accounts]

I grant my executor full access to both the catalogue and the content of electronic communications sent or received by me to the fullest extent allowed under state and federal law. [The e-mail addresses of these accounts include but are not limited to: _____.]

[full access to some accounts]

I grant my executor full access to both the catalogue and the content of electronic communications sent or received by me to the fullest extent allowed under state and federal law limited to the following e-mail addresses: _____].

[partial access to all accounts]

I grant my executor the right to receive and access the catalogue of electronic communications sent or received by me to the fullest extent allowed under state and federal law. [The e-mail addresses of these accounts include but are not limited to: _____.] However, my executor has no right to receive access to the content of any electronic communication sent or received by me.

[partial access to all some accounts]

I grant my executor the right to receive and access the catalogue of electronic communications sent or received by me to the fullest extent allowed under state and federal law limited to the following e-mail address: _____. However, my executor has no right to receive access to the content of any electronic communication sent or received by me.

[no access]

My executor does not have any right to receive the catalogue or content of any electronic communications sent or received by me [except if required to comply with tax laws or other legally enforceable requirements or obligations].

2. Long Form Sample 1

[Adapted from a provision supplied by James Lamm and reproduced in Michael Froomkin, *Estate Planning for Your Digital Afterlife*, Discourse.net (Feb. 18, 2013).]

The personal representative may exercise all powers that an absolute owner would have and any other powers appropriate to achieve the proper investment, management, and distribution of: (1) any kind of

computing device of mine; (2) any kind of data storage device or medium of mine; (3) any electronically stored information of mine; (4) any user account of mine; and (5) any domain name of mine. The personal representative may obtain copies of any electronically stored information of mine from any person or entity that possesses, custodies, or controls that 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 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; (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 Electronic Communications Privacy Act of 1986, 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. The personal representative may employ any consultants or agents to advise or assist the personal representative in decrypting any encrypted electronically stored information of mine or in bypassing, resetting, or recovering any password or other kind of authentication or authorization, and I hereby authorize the personal representative to take any of these actions to access: (1) any kind of computing device of mine; (2) any kind of data storage device or medium of mine; (3) any electronically stored information of mine; and (4) any user account of mine. 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.

3. Long Form Sample 2

[Adapted from Michael D. Walker, *The New Uniform Digital Assets Law: Estate Planning and Administration in the Information Age*, 52 REAL PROP, TR., & EST. L.J. 51, 75 (2017).]

(a) My Personal Representative may take any action (including, without limitation, assuming or amending a terms-of-service agreement or other governing instrument) with respect to my Digital Assets, Digital Devices, or Digital Accounts as my Personal Representative shall deem appropriate, and as shall be permitted under applicable state and Federal law. My Personal Representative may engage experts or consultants or any other third party, and may delegate authority to such experts, consultants or third party, as necessary or appropriate to effectuate such actions with respect to my Digital Assets, Digital Devices, or Digital Accounts, including, but not limited to, such authority as may be necessary or appropriate to decrypt electronically stored information, or to bypass, reset or recover any password or other kind of authentication or authorization. This authority is intended to constitute "lawful consent" to any service provider to divulge the contents of any communication or record under The Stored Communications Act (currently codified as 18 U.S.C. §§ 2701 et seq.), the Computer Fraud and Abuse Act (currently codified as 18 U.S.C. § 1030), and any other state or federal law relating to Digital Assets, data privacy, or computer fraud, to the extent such lawful consent may be required. My Personal Representative shall be an authorized user for purposes of applicable computer-fraud and unauthorized-computer-access laws. The authority granted under this paragraph is intended to provide my Personal Representative with full authority to access and manage my Digital Assets, Digital Devices, or Digital Accounts, to the maximum extent permitted under applicable state and Federal law and shall not limit any authority granted to my Personal Representative under such laws.

(b) The following definitions and descriptions shall apply under this will to the authority of the Personal Representative with respect to my Digital Assets and Accounts:

(1) "Digital Assets" shall be any electronic record that is defined as a "Digital Asset" under the [applicable state law], together with any and all files created, generated, sent, communicated, shared,

received, or stored on the Internet or on a Digital Device, regardless of the ownership of the physical device upon which the digital item was created, generated, sent, communicated, shared, received or stored (which underlying physical device shall not be a "Digital Asset" for purposes of this will).

(2) A "Digital Device" is an electronic device that can create, generate, send, share, communicate, receive, store, display, or process information, including, without limitation, desktops, laptops, tablets, peripherals, storage devices, mobile telephones, smart phones, cameras, electronic reading devices, and any similar digital device which currently exists or may exist as technology develops or such comparable items as technology develops.

(3) "Digital Account" means an electronic system for creating, generating, sending, sharing, communicating, receiving, storing, displaying, or processing information which provides access to a Digital Asset stored on a Digital Device, regardless of the ownership of such Digital Device.

(4) For the purpose of illustration, and without limitation, Digital Assets and Digital Accounts shall include email and email accounts, social network content and accounts, social media content and accounts, text, documents, digital photographs, digital videos, software, software licenses, computer programs, computer source codes, databases, file sharing accounts, financial accounts, health insurance records and accounts, health care records and accounts, domain registrations, DNS service accounts, web hosting accounts, tax preparation service accounts, online store accounts and affiliate programs and other online accounts which currently exist or may exist as technology develops, or such comparable items and accounts as technology develops, including any words, characters, codes, or contractual rights necessary to access such items and accounts.

B. Power of Attorney

[Adapted from Keith P. Huffman, *Law Tips: Estate Planning for Digital Assets*, Indiana Continuing Legal Education Forum (Dec. 4, 2012)

Digital Assets. My agent has (i) the power to access, use, and control my digital device, including, but not limited to, desktops, laptops, peripherals, storage devices, mobile telephones, smart phones, and any similar device which currently exists or exists in the future as technology develops for the purpose of accessing, modifying, deleting, controlling or transferring my digital assets, (ii) the power to access, modify, delete, control, and transfer my digital assets, including, but not limited to, any emails, email accounts, digital music, digital photographs, digital videos, software licenses, social network accounts, file sharing accounts, financial accounts, domain registrations, web hosting accounts, tax preparation service accounts, on-line stores, affiliate programs, other on line programs, including frequent flyer and other bonus programs, and similar digital items which currently exist or exist in the future as technology develops, and (iii) the power to access the content of all electronic communications as defined by [citation to state statute].

C. Authorization and Consent for Release of Electronically Stored Information

[Adapted from Wealthaven, LLC, *Sample Digital Language* (2014).]

By this document, I hereby authorize and consent for any person or entity that has possession, custody or control over any electronically stored information or digital assets wherein I have a property right or interest, or that provides an electronic communication service, a remote communication service, a storage service, whether public or private, to release and disclose to my personal representatives (a) any electronically stored information, (b) the contents of any communication that is in electronic storage by that service or that is carried or maintained on that service, (c) any record or other information pertaining to me with respect to that service.

It is my intention that this authorization and consent is to be construed as broadly as possible to allow my personal representative under this document to have the access and use of information described above. I intend for my personal representative to include a trustee of my revocable trust, a trustee of a trust appointed under my will, an attorney in fact (agent) acting under a power of attorney document, a guardian or conservator appointed for me, the personal representative or executor of my estate or other representative created by operation of law.

This authorization and consent is to be construed to be my lawful consent under the Electronic Communications Privacy Act of 1986, as Amended; the Computer Fraud and Abuse Act of 1986 as amended; and any other applicable federal or state data privacy or criminal law.

This authorization is effective immediately. Unless I revoke this authorization 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, 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.

D. Non-Authorization

[Adapted from Jennifer J. Wioncek & Michael D. Melrose, *Executive Summary* (May 10, 2016).]

My [type of fiduciary such as executor or agent] does not have any right to receive the catalogue or content of any electronic communications sent or received by me.

[or]

My [type of fiduciary such as executor or agent] has the right to receive and access the catalogue of electronic communications sent or received by me. However, my [type of fiduciary such as executor or agent] shall have no right to receive access to the content of any electronic communication sent or received by me.

E. Pleading

Applicant, the personal representative of the Estate of [name of deceased], respectfully requests the court to make the following findings:

1. [Name of deceased] had the following account with [name of custodian] identified as follows:
    - Account number: _____.
    - User name: _____.
    - Address: _____.
    - Unique subscriber or account identifier: _____.
2. Disclosure of the content of this account would not violate 18 U.S.C. § 2701 et seq., 47 U.S.C. § 222, or other applicable law.
3. [Name of deceased] expressly consented to the disclosure of the content of an electronic communication in [his/her] will.

4. Disclosure of the content of [name of deceased] electronic communication is reasonably necessary for the administration of [name of deceased]'s estate.

F. Court Order

The court finds the following:

1. Applicant is the personal representative of the Estate of [name of deceased].
2. [Name of deceased] had the following account with [name of custodian] identified as follows:
    - Account number: _____.
    - User name: _____.
    - Address: _____.
    - Unique subscriber or account identifier: _____.
3. Disclosure of the content of this account would not violate 18 U.S.C. § 2701 et seq., 47 U.S.C. § 222, or other applicable law.
4. [Name of deceased] expressly consented to the disclosure of the content of an electronic communication in [his/her] will.
5. Disclosure of the content of [name of deceased] electronic communication is reasonably necessary for the administration of [name of deceased]'s estate.

APPENDIX C – SAMPLE REQUEST LETTER TO DIGITAL ASSET CUSTODIAN

[Adapted from Michael D. Walker, *The New Uniform Digital Assets Law: Estate Planning and Administration in the Information Age*, 52 REAL PROP, TR., & EST. L.J. 51,77 (2017).]

Via Certified Mail _____
Return Receipt Requested

Cyberdyne Systems
1701 Enterprise Drive
Skynet, CA 90210

Re: Email Account of Sarah Connor, Deceased (iwantolive@cyberdyne.com)

Dear Custodian:

I am the duly appointed personal representative of Sarah Connor (the "Decedent"). The Decedent died on _____.

Pursuant to the [citation to state's version of RUFADAA] (hereafter, "RUFADAA"), I hereby request full access to the Decedent's email account maintained by Cyberdyne Systems. In connection with this request, I am enclosing the following:

1. A certified copy of the death certificate of the Decedent.
2. A certified copy of the Letters Testamentary issued by [court] on [date] which appoints me as the Personal Representative of the Decedent's estate.
3. A copy of the Will of Decedent dated [date]. Please note that pursuant to [citation to enabling will provision] of the Decedent's Will, the Decedent expressly provided her full consent to the disclosure of all her digital assets, including the content of electronic communications, to her personal representative, and further authorized her personal representative to take any and all actions relating to her digital assets as her personal representative shall deem appropriate.
4. A copy of an email dated [date] which was sent to me by the Decedent. This email contains the Decedent's cyberdyne.com email address referenced above, together with other information identifying the Decedent's account with Cyberdyne Systems.

I look forward to your prompt response in accordance with RUFADAA. Please contact me if you have any questions.

Very truly yours,

Kyle Reese
Personal Representative
Estate of Sarah Connor, Deceased

APPENDIX D – A PRIMER FOR PROBATE JUDGES

Originally published in NAT'L COLLEGE OF PROB. JUDGES J., Fall 2017, at 1
(slightly edited to update)

A new type of motion is going to start hitting your bench with increased frequency – a request for an order allowing the personal representative to access a decedent's or ward's digital assets. What is this all about? What do I need to know? Should I grant or deny the motion? This article aims to answer these and other questions so that probate judges are well-informed about the cyberspace-estate administration interface.

What is a digital asset?

Digital assets are electronic records (think binary 1s and 0s) in which a person has a right or interest. Examples include e-mails, text messages, photos, digital music and video, word processing documents, social media accounts (e.g., Facebook, LinkedIn, Twitter), and gaming avatars.

Why does a personal representative care about the digital assets of a decedent?

There are many reasons why a personal representative would want access to the decedent's digital assets. (1) Many people forego paper statements for financial accounts such as bank accounts, retirement accounts, and brokerage accounts. The personal representative may seek access to the contents of the decedent's e-mail messages to ascertain where these accounts are located and to gain the information necessary to complete the estate inventory, pay creditors, and distribute the funds appropriately. (2) Likewise, many people forego paper statements for utilities, credit cards, car loans, and home mortgages. The personal representative may need to give notice to and pay these creditors and thus needs access to e-mail messages to determine the names of the creditors and the amounts owed. (3) Some digital assets like domain names, customer lists, manuscripts, and compositions may have significant economic value. The personal representative needs access to these assets for both inventory and distribution purposes. (4) Some digital assets like family photos and videos do not have monetary value but they have great sentimental value and need to be transferred to the proper heirs or will beneficiaries.

What law governs a personal representative's access to digital assets?

See Appendix E, page 61.

Does it matter when the decedent died?

No. RUFADAA applies to a personal representative acting for a decedent who died before, on, or after the effective date.

How is priority for access to a decedent's digital assets determined?

Section 4 of RUFADAA provides the priority order. First priority is given to the decedent's instructions using the custodian's online tools. Examples include Google's Inactive Account Manager and Facebook's Legacy Contact. Second priority is given to the decedent's instructions in the decedent's will. If the decedent has not provided instructions through an online tool or will, then the service provider's terms of service agreement (the "I agree' button) will govern the rights of the decedent's personal representative.

Is there anything special about "access" that I need to know?

Yes! There is a major difference between two types of access. The first type is access to the contents of electronic communications which refers to the substance or meaning of the communication such as the actual subject line and text of e-mail messages.

The second type of access encompasses both the catalogue of electronic communications (e.g., the name of sender, the e-mail address of the sender, and the date and time of the message but *not* the subject line or the content) and other digital assets (e.g., photos, videos, material stored on the decedent's computer, etc.).

Why is the personal representative bothering me for a court order?

RUFADAA §§ 7 & 8 provide procedures for the personal representative to seek access to digital assets directly from the custodian without the need for a court order. However, the custodian is authorized to ask for a court order before granting access. Many custodians ask for a court order as a matter of standard practice.

What must a court order granting access to contents of electronic communications contain?

You must make the following findings in your court order to grant the executor access to the contents of electronic communications:

- The decedent had the specific account with the custodian including the account's number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the decedent's account.
- The disclosure of the contents would not violate 18 U.S.C. § 2701 et seq., 47 U.S.C. § 221, or other applicable law.
- The decedent expressly consented in the decedent's will to the disclosure of the contents.

May I issue a court order granting access to contents of electronic communications if the decedent died intestate or did not authorize access in the decedent's will?

From a practical point of view, no. You should issue a court order granting access to contents only if the decedent had a will which expressly authorized the executor to have access to contents. From the exact terms of the statute, however, you have the power to issue the order even without permission but evidence shows the custodian will balk at such an order.

What must a court order granting access to the catalogue of electronic communications and other digital assets contain?

You must make the following findings in your court order to grant the executor of a will or the administrator of an intestate estate access to the catalogue of electronic communications and other digital assets:

- The decedent had the specific account with the custodian including the account's number, username, address, or other unique subscriber or account identifier assigned by the custodian to identify the decedent's account.
- The disclosure is reasonably necessary for the administration of the estate.

How long does the custodian have to comply with my court order?

The custodian should comply with the request not later than 60 days after your order under RUFADAA § 16. However, a custodian incurs no penalty for failing to disclose within sixty days of a proper request. If the custodian does not disclose, the personal representative may apply to your court for an order directing compliance. This order must state that compliance is not in violation of 18 U.S.C. § 2702. The decedent's

estate bears all the expenses of seeking and obtaining the court order such as attorney fees and court costs. If the custodian does not comply with the court order, you may be able to make an award against the custodian for non-compliance expenses or contempt of court.

Might I need to deal with digital assets in a guardianship or conservatorship?

Yes. Because a protected person is likely to retain a right to privacy in personal communications, access to digital assets is not automatically granted to a guardian or conservator by virtue of the fact that the person is appointed as a guardian or conservator.

If there is a hearing on the matter, you may grant a guardian complete access to the ward's digital assets, that is, the contents of electronic communications, the catalogue of electronic communications, and other digital assets in which the ward has a right or interest. RUFADAA § 14(a).

Without a hearing, a guardian may obtain access to the catalogue and digital assets other than the content of electronic communications but a court order is still required along with other specified required documentation including a certified copy of the court order that granted the guardian authority over the ward's digital assets. RUFADAA § 14(b).

A guardian may also request that an account be terminated or suspended for good cause upon providing the custodian with a copy of the court order giving the guardian general authority over the protected person's property. RUFADAA § 14(c).

Might I need to deal with digital assets when a power of attorney or trust is involved?

Yes. A custodian has no right to ask for court findings as is the case when a personal representative of a decedent's estate is involved. However, if the custodian does not comply with an agent or trustee's valid request, the agent or trustee may seek a court order requiring the custodian to comply with the disclosure request.

Where can I get more information about RUFADAA?

RUFADAA has extensive Comments which are very helpful. You may access them on the website of the Uniform Law Commission at http://www.uniformlaws.org/.

You may also access a comprehensive article on the planning for and administration of digital assets at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2166422.

APPENDIX E – SUMMARY OF STATE STATUTES

A. RUFADAA Enacted

1. Alabama. Chapter 1A of Title 19, Code of Alabama 1975
2. Alaska. HB 108. Will be Alaska Stat.§ 13.26.645
3. Arizona. Ariz. Rev. Stat. §§ 14-13101 et seq.
4. Arkansas. 28 Ark. Stat. Ch. 75
5. California. SB 1458 amending Calif. Prob. Code §§ 870 et seq.
6. Colorado. Colo. Rev. Stat. §§ 15-1-1501 et seq.
7. Connecticut. Conn. Gen. Stat. § 45a-334b et seq.
8. District of Columbia. D.C. Code §§ 21-2501-21-2518.
9. Florida. Fla. Stat. §§ 740.001 et seq.
10. Georgia. SB 301.
11. Hawaii. Hawaii Rev. Stat. §§ 556A-1 et seq.
12. Idaho. Idaho Code §§ 15-14-101 et seq.
13. Illinois. 755 ILCS 70/1 et seq.
14. Indiana. Ind. Code Ann. § 32-39-1-1 et seq.
15. Iowa. 2017 S.B. 333.
16. Kansas. 2017 S.B. 63.
17. Kentucky: Ky. Rev. Stat. Ch. 395A
18. Maine. LD 846.
19. Maryland. Md. Estates & Trust Code §§ 15-601 et seq.
20. Michigan. Mich. Comp. Laws §§ 700.1001 et seq.
21. Minnesota. Minn. Stat. §§ 521A.01 et seq.
22. Mississippi. 2017 H.B. 849.
23. Missouri. Mo. Stat. 472.400-472.490.
24. Montana. 2017 S.B. 118.
25. Nebraska. Rev. Stat. Neb. §§ 30-501 to -518.
26. Nevada. AB 239. Title 59 Nev. Rev. Stat. (new chapter).
27. New Hampshire. Ch. 554-A.
28. New Jersey. A3433. Title 3B C.3B:14-61.
29. New Mexico. 2017 S.B. 60.
30. New York. McKinney's EPTL §§ 13-A-1 to 13-A-5.2.

31. North Carolina. N.C. Gen. Stat. §§ 36F-1 et seq.
32. North Dakota. Chapter 47-36 of the North Dakota Century Code.
33. Ohio. Ohio Rev. Code §§ 2137.01 et seq.
34. Oklahoma. Okla. Stat. tit. 58, § 3101 et seq.
35. Oregon. 2016 S.B. 1554.
36. Pennsylvania. 20 Pa. Cons. Stat. Ch. 39.
37. Rhode Island. Title 33, Ch. 27.1.
38. South Carolina. S.C. Code Ann. §§ 62-2-1010 et seq.
39. South Dakota. 2017 H.B. 1080.
40. Tennessee. Tenn. Code §§ 35-8-101 et seq.
41. Texas. Tex. Est. Code Ch. 2001.
42. Utah. 2017 H.B. 13.
43. Vermont. 2017 H.B. 192, Act 13.
44. Virginia. 2017 H.B. 1608, Chap. 33 / 2017 S.B. 903, Chap. 80
45. Virgin Islands. 15 V.I. Code ch. 65
46. Washington. Rev. Code Wash. §§ 11.120.010 et seq.
47. West Virginia. W. Va. Code § 44-5B-1 et seq.
48. Wisconsin. Wisc. Stat. § 711.01 et seq.
49. Wyoming. Wyo. Stat. § 2-3-1001 et seq.

B. RUFADAA Pending

Massachusetts.

C. Non-RUFADAA

1. Delaware. Del. Code tit. 12 § 5001 to 5007 (UFADAA)
2. Louisiana. La. Code of Civ. Proc., Art. 3191.