

The Basics of Digital Asset Planning and Administration

Presented by:
Bruce D. Hendryx – PNC Asset Management Group

Digital Assets: The challenges of Planning, Administration, Asset Gathering and Asset Disposition

I. Introduction:

A fiduciary is charged with protecting assets of the beneficiaries for whom the assets represent value. Planning that does not adequately coordinate with user tools and contractual language for site usage can create significant disconnects once the estate is under administration. The fiduciary must gather and protect those assets and once collected, the next goal is to make those assets productive (and perhaps protect the estate from diminution of those assets). In making the decisions, the fiduciary document is the guidepost. When those assets prove to be difficult to identify, to value, or to custody, the role of the fiduciary becomes even more difficult (and even precarious).

The Goals of this presentation therefore will be to:

- 1) Define Digital Assets;
- 2) Discuss Planning Strategies;
- 3) Explain the duty of the fiduciary; and,
- 4) Insert statutory guidance around these assets.

Digital Assets present a very specific problem. By their very nature in some cases, they may be difficult to hold and administer. For Digital Assets with apparent economic value, it may be difficult to realize that value. Other Digital Assets may be of no cash value at all.

Digital Assets are growing RAPIDLY. Just consider the growth of the internet and a sample of technology companies.

A timeline of digital events:

- Birth of internet¹
 - o 1960's – Governmental Use (ARPANET)
 - o 1983 – Commercial application (TCP/IP)
- Selling/Social Media on the Internet:
 - o 1995 - EBay (AuctionWeb) started
 - o 2002 – Ebay acquires PayPal
 - o 2004 – Facebook launches. As of 2017 over 2 billion active users.²
 - o 2006 – Twitter launches³
 - o 2010 – Instagram launches⁴
 - o 2017 – Social Media/E-Commerce and Conversion Statistics⁵
 - *“The e-commerce industry is responsible for about \$2 trillion in annual sales.”*
 - *“Worldwide B2C e-commerce sales reached \$1.7 trillion in 2015, and it is estimated to reach \$2.35 trillion by 2018.”* Note: This is a projected increase of 17.5% for 2018.
 - *“There are 2.79 billion active social media users in the world. This is an increase of 21 percent from 2016.”*

¹ A Brief History of the Internet, http://www.usg.edu/galileo/skills/unit07/internet07_02.phtml

² <https://en.wikipedia.org/wiki/Facebook>

³ https://en.wikipedia.org/wiki/Timeline_of_Twitter

⁴ <https://instagram-press.com/blog/2010/10/06/instagram-launches-2/>

⁵ <https://hostingfacts.com/internet-facts-stats-2016/>

- 2021 - Social Media/E-Commerce and Conversion Statistics⁶
 - *There are 7.83 billion people in the world. (Worldometer), 4.66 billion of them are active Internet users. (Statista)*
 - *There are 4.14 billion active social media users around the globe. (Statista)*
 - *Retail eCommerce sales are projected to grow to 6.54 trillion US dollars in 2022. (Statista)*

From this point forward, we will use the framework of the UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT, REVISED (2015) (hereinafter UFADAA) to frame the discussion on how a fiduciary should consider Digital Assets. Section 2 of UFADAA provides critical definitions which follow below.

II. Defining Digital Assets:

Revised Uniform Fiduciary Access to Digital Assets Act (UFADAA) defines digital assets. “Digital asset means 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.”⁷

UFADAA also helps Fiduciaries understand the rules which govern access to a person's online accounts when the account owner dies or loses the ability to manage the account. It should be noted however, if an underlying asset is itself an electronic record, the electronic record in which the individual has a right or interest is a Digital Asset.

Examples of Digital Assets which are Electronic Records:

- 1) An e-mail, image or photograph which is saved on a smartphone, computer, website or perhaps a cloud account.
- 2) Domain names, digital music, digital literature or digital art.
- 3) Digital Assets may simply be electronic information about tangible assets. For example, the Digital Asset could be an electronic statement for a checking account at a local bank.
- 4) Non-Fungible Tokens (NFTs) – Artwork or another form of symbolism which is unique or limited and thus has value.
Example: Digital Artwork for games, websites or other online sources which can only be found digitally.
- 5) Digital Assets also include cryptocurrencies.

An example would be Bitcoin, Ethereum, Dogecoin or over 20,000 others. Cryptocurrency is not tangible and only exists as an electronic record.

Under UFADAA, “. . . “digital asset” expressly excludes underlying assets such as funds held in an online bank account.”⁸

Cryptocurrency:

Cryptocurrency is virtual currency. The IRS defines virtual currency as “an example of a convertible virtual currency that can be used as payment for goods and services, digitally traded between users, and exchanged for or into real currencies or digital assets.”⁹ According to Wikipedia, “a cryptocurrency is a digital or virtual currency that uses cryptography for security.”¹⁰ The reaction of the public, the marketplace and regulatory

⁶ <https://hostingfacts.com/internet-facts-stats/>

⁷ UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT, REVISED (2015) (UFADAA), p4

⁸ UFADAA, p6

⁹ [Digital Assets | Internal Revenue Service \(irs.gov\)](https://www.irs.gov/digital-assets)

¹⁰ <https://www.investopedia.com/terms/c/cryptocurrency.asp>

authorities to cryptocurrency, whether negative or positive, may be regarded as developing, on-going and variable. It is beyond the scope of this presentation to address cryptocurrency other than as an illustration of a type of Digital Asset. It should not be regarded as an endorsement.

Below is a summary of certain statistics regarding cryptocurrency.¹¹ As noted below, we can also see the intense volatility of these assets and the commensurate risk.

| Cryptocurrencies (including Bitcoin) Market Information | | | | |
|---|-------------------|----------------------|----------------------|------------|
| | Information as of | | Difference | Pct Change |
| | 12/31/2013 | 12/31/2022 | | |
| All Cryptocurrencies | | | | |
| Market Capitalization | 10,059,549,969.00 | 1,045,987,345,470.00 | 1,035,927,795,501.00 | 10297.95% |
| Number of Cryptocurrencies | 66 | 22,354 | 22,288 | 33769.70% |
| Bitcoin | | | | |
| Price | \$724.05 | \$22,989.13 | \$22,265.08 | 3075.07% |

What we should know: Again, the reference point to address Fiduciaries’ specific concerns regarding Digital Assets, for purposes of this presentation, is UFADAA as enacted by various state legislatures. In those states where it has not been adopted, it may be a useful reference point.

III. Planning:

Clients need to understand their digital footprint. The vast majority of Americans have digital assets. Things like Airline mile programs, retail point plans and other like-kind items are digital assets.

- Some of these are not significant in overall value. However, others have the potential to be very large. PayPal balances, Crypto balances, etc.
- Are these individuals Gamers, Gamblers, Social Networkers, Collectors (Anime’ and other forms of digital collections)?

To Do’s for Clients:

- Does the client’s intended Executor/Trustee have the desire, expertise, ability to act for these digital assets? If not,
 - o Consider a Separate Fiduciary for Digital Assets; and/or,
 - o A directing party for digital assets
- Does your Client want their heirs to have access to all, some or none of their digital data/assets?
 - o UFADAA preference: Privacy is presumed unless decedent directs differently.
 - o Clients’ intentions need to be clear
- Coordination with User Agreements
 - o Online Tools – Frequently Address access. This must be coordinated or custodians will not allow.
 - o Have Client name the Fiduciary as an Authorized User in the Fiduciary Documents and in User Agreements.
 - o User Agreements – may restrict access, thus important to provide clear guidance
 - o License Agreements – may only create a life-estate
- Layout a list of all electronic/digital assets.
 - o Some assets may have great sentimental value but little economic value

¹¹ <https://coinmarketcap.com/all/views/all/>

- Be clear about those with monetary value and those with emotional value
- Be very clear about those items that shall remain private.
- Provide guidance around password management tools
 - If clients use a password management software,
 - What is the Password Management software?
 - Does it work with all of their data?
 - Does the service allow the Password Management Software to provide that information to someone else in the event of your passing?
 - Define clearly who has that right. Are there succession options for that role?
 - Written passwords. Are your passwords written somewhere that is secure?
 - Note who has access to the passwords
 - Is that location accessible?
- Your Phone is often the gateway to all other devices.
 - What about the password to your phone?
 - Ensure another party has the means to enter that password.
 - Consider having another party who can rescue the phone.
 - If you use Face ID, who can access?
 - Upon death/disability: Don't immediately shut it off!
- Where are the client's digital assets?
 - On the Cloud? Are they connected to your Apple account or some other service?
 - If so, at death, what does your Service/User's Agreement say about access?
 - Important to check all online access for that information.
 - Understand how you access data:
 - Apple Devices: Provide for a Legacy Contact who can access your data at your death. Ensure that phones, computers and tablets are coordinated on this.
 - Android Devices: Allow very limited access to family members unless the user provides access via Google's Inactive Account Manager.
- Work with clients to create directives to maintain phone, cloud and other data services after death to ensure that you do not lose data.
- Ensure that clients provide the planner and the Fiduciary all services they use.
 - For planners: important to determine whether they can preserve access rights under user agreements (in advance).
 - For Fiduciaries: important to reach out to access and enforce those access rights.
 - Examples: Facebook(Meta); Instagram; Twitter; LinkedIn;
- Help Clients understand that 2-factor Authentication may cause issues.
 - Ensure that the device is still active (normally a phone/text process or email completes that Authentication) and
 - is accessible to your Fiduciary.
- Most Important: Tell the Fiduciary/Party who will act for you that they are being named. Make sure they are willing to act!

IV. Oversight for Digital Assets - Fiduciaries:

Fiduciaries should consider addressing the unique nature of these assets and possible constructs to create policies/procedures, utilize experts for that oversight and create risk management processes to ensure consistency. The list below may help set forth those considerations:

The details herein are for information purposes only and are not to be relied upon as tax or legal advice.



- Expertise
 - o Do you have internal experts who can identify the risk issues?
 - o If you don't have internal experts can or should you hire/delegate these responsibilities?
 - o Is the Estate/Trust Document appropriate for the assets you will receive?
 - o Can you store/custody the asset?
 - Digital Assets and their related Electronic Devices create many risk issues.
 - Electronic Devices include: Computers, CDs, other data disks, USB storage, Flash Drives, etc.
- System Capabilities:
 - o Do you have systems in place (e.g., for assets having value)?
 - o Can or should you use a supplemental system?
- Risk Management –
 - o What type of Risk Management process is in place?
 - o Committee Structure – Investment and Fiduciary Risk
 - o Have protocols/guides or policies/procedures been developed?
 - Are there guidance and oversight standards for these assets?
 - How do you analyze
 - Practicalities
 - Risk
 - Valuation
 - Review
 - Fees

Consider Risk:

- Understanding the Risk:
 - o Operational Risk – Risk due to poor controls/systems
 - A huge factor is the risk of accidental deletion of service.
 - The Phone is often the most important tool for access to data. Protect it.
 - o Compliance Risk – Risk for failure to follow legal requirements
 - o Strategic Risk – Risk of over-extending oneself
 - o Reputational Risk – Risk to reputation for failing to oversee
- Find Ways to Mitigate Risk:
 - o Create and constantly update your risk management/oversight system
 - o Ensure that it is robust and open ended for inquiry and adjustment
 - o Empower/fund the areas that will oversee these assets
 - o Ensure Risks can be assessed – Quantify those risks.
 - o Create Risk Controls – Protocols/Guidelines, Policies/Procedures, systems/internal oversight
 - Review at acceptance/ongoing review

Applying UFADAA to the Oversight of Digital Assets

These risk management tools then must be addressed in the context of the unique considerations for Digital Assets.

- Know that different fiduciary roles may influence different solutions.
- Understand the unique characteristics and growth of Digital Assets.

- Recognize the potential impact of governing documents (e.g., Will/Trust/On-Line Tool/Terms of Service Agreement) and the Law.
- Create and enforce a Robust Legal Review Process

For fiduciaries who have accepted the role of fiduciary for a decedent or incapacitated party, the applicability of UFADAA is determined under UFADAA Section 3¹² below.

Section 3) Applicability. Applies to various fiduciary situations:

- Fiduciary acting under a will or POA
- Personal Representative acting for a decedent
- Conservator or Guardian
- Trustee

For example, in the case of a Decedent's Estate, has the Decedent made a provision for the allowance or prohibition of disclosure to the Fiduciary of some or all of the Decedent's Digital Assets, including the content of electronic communications sent or received by the Decedent? If so, the question is, how did the Decedent make that provision? Sections 4 – 5¹³ address these conflicts.

Section 4) User Direction for Disclosure of Digital Assets.

- ONLINE TOOL EXISTS (Has User taken the time to address these issues?):
If User has directed the Custodian via an online tool to allow or disallow the disclosure of information to a designated recipient, the direction will OVERRIDE a contrary direction in the will, trust or POA if the online tool allows the User to modify or delete a direction at all times.
- ONLINE TOOL EXISTS (User has not used it) OR NO ONLINE TOOL EXISTS:
User may so allow or prohibit such disclosure in a will, trust, POA or other record.
- User's direction in a. or b. overrides a contrary provision in a Terms of Service Agreement that does not require the User to act affirmatively and distinctly from the User's assent to the Terms of Service. Otherwise, Terms of Service provisions apply.

Section 5) Terms of Service Agreement.

- UFADAA does not change rights of Custodian or user to access and use Digital Assets of the user.
- UFADAA gives no new rights to Fiduciary or designated recipient other than those held by the User.
- Fiduciary's or designated recipient's access to Digital Assets may be modified or eliminated by User, Federal Law or Terms of Service Agreement if User has not provided direction under Section 4.

Factors related to UFADAA provisions:

- 1) Determine if the will/trust provides for disposition/protection of the Digital Asset?
- 2) Determine if will/trust contains a direction to allow or disallow the disclosure of information to the Fiduciary.
 - Does the Terms of Service Agreement apply?
 - What rights might the fiduciary have to protect and access those assets?

¹² UFADAA, pp 8-10

¹³ UFADAA, pp 10-12

- If the Custodian provides for Online Tools and the User (protected party) has:
 - a. Provided rights to the fiduciary or other parties to access these electronic records, the Custodian should grant access accordingly.
 - b. Directed that no access be granted, presumably the Custodian will not grant access.
 - If the Online Tools are not filled out or do not exist then direct language in the fiduciary document will be considered.
- 3) Consider other laws:
- o Fiduciary Laws (obligation of fiduciary to preserve value of the assets of a trust/estate).
 - UFADAA: “Revised UFADAA gives states precise, comprehensive, and easily accessible guidance on questions concerning fiduciaries’ ability to access the electronic records of a decedent, protected person, principal, or a trust.”¹⁴
 - o Privacy Laws (protecting the rights of the decedent to privacy even after death)
 - o Hacking Laws (protecting consumers from someone accessing accounts for which they have no right)
 - Electronic Communications Privacy Act (ECPA)¹⁵, is legislation which limits access to communications of a User without authority. The protection of privacy is a major factor in cases involving Digital Assets. See also Computer Fraud and Abuse Act.¹⁶
- 4) Note protected interests: The key piece of information which is protected is the user’s “content” which includes information in the body of an electronic communication that is “not readily accessible to the public. . . .”¹⁷
- For example: an email, Facebook or Twitter communication that is limited to one or a limited number of recipients is deemed protected. However a public communication (where anyone can see the communication) is not protected.
- 5) Consider options for obtaining information:
- a. **Communication Log:** If a Custodian declines to provide the Fiduciary with access to electronically stored communications, the Fiduciary may seek a log of communications (e.g., a log of emails stating the sender, recipient, date and time).
 - b. **Online Tool:** An online tool may be a consideration for oversight of an account. An online tool is defined in Section 2. of UFADAA as “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.” It is also described as “a mechanism by which a user names an individual to manage the user’s digital assets after the occurrence of a future event, such as the user’s death or incapacity. The named individual is referred to as the “designated recipient” in the act to differentiate the person from a fiduciary. A designated

¹⁴ UFADAA, p2

¹⁵ Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. Section 2701

¹⁶ 18 U.S.C., Section 1030

¹⁷ UFADAA, p6

recipient may perform many of the same tasks as a fiduciary, but is not held to the same legal standard of conduct.”¹⁸

Thus, if a person anticipates his or her demise and, through an online tool, names a designated recipient to have full access, the designated recipient would have the ability to access those records covered by the online tool. It is advisable to know the law and legal obligations prior to access.

- c. **Employer Property:** Note, if a Digital Asset is the property of the Employer of the decedent/protected party, the Digital Asset is NOT covered by UFADAA¹⁹.
- d. **Application of Law:** UFADAA applies to Custodians based on the state in which that party resided at the time (where UFADAA was enacted) the event occurred (death, transfer to IRREV Trust, etc).²⁰

Next: Consider the steps for accessing these Digital Assets. Query whether the Custodian will seek to block access.

Section 6) PROCEDURE FOR DISCLOSING DIGITAL ASSETS.

Custodian

- a. May at its **sole discretion**:
 - o Grant full access
 - o Grant partial access (to meet fiduciary’s duties)
 - o Provide a copy of a Digital Asset that the user could have accessed if the user was able to do so
- b. May assess a reasonable administrative charge.
- c. Need not disclose a Digital Asset deleted by user.
- d. If only some Digital Assets are to be disclosed, no need to disclose if “undue burden”.
However, Custodian or fiduciary can seek a court order to disclose:
 - o All, some or none of the items.
 - o A private (or in camera) review of all Digital Assets in front of the court can also be requested.

Disclosing Digital Assets: The Custodian is charged with protecting those assets²¹.

- **Query whether a Custodian will require a Court Order to protect against claims.**
- **The requests for information should be specific.**
- **Query whether a User’s direction in an online tool or the fiduciary document provide for disclosure.**

Accessing Content vs. Non-Content Communications:

Definition:

¹⁸ UFADAA, p8

¹⁹ UFADAA, p9

²⁰ UFADAA, p9

²¹ 18 U.S.C. Section 2702 (a)

Content Based Communication: the actual communications by a party within private emails or other private electronic communications.

Non-Content Based Communication is a catalogue showing that a private email was sent with dates/times and recipient information (but not the actual text of the communication).

The following sections relate to access to Content-Based communications vs. Non-Content Based Communications. Access is very limited within UFADAA. Under federal law, the main issues are that Content-Based communications require “lawful consent”²². UFADAA provides for Fiduciary access to Content-Based communications and Non-Content communications under only certain circumstances as described in the statute.²³

Estates (Sections 7-8)²⁴

SECTION 7. DISCLOSURE OF CONTENT OF ELECTRONIC COMMUNICATIONS OF DECEASED USER.

If User consented to or if a court orders disclosure, Custodian shall disclose if the representative of the Estate gives:

- 1) Written request
- 2) Certified copy of death certificate
- 3) Legal Docs (court order, letter of appointment, etc.)
- 4) Copy of will, trust, POA, etc, (unless User provided access by User Tool)
- 5) Custodian may request that the Estate representative provide:
 - a. Acct identifiers
 - b. Evidence to link user to the account
 - c. Court finding
 - i. That gives a and b
 - ii. Confirmation that disclosure does not violate law (including Unlawful Access to Stored Communications)²⁵
 - iii. If User Consent was not from an online tool, provision of user consent
 - iv. Disclosure is reasonably necessary for administration of the Estate

Query whether a Custodian will require a court order when the User has directed that the Fiduciary have access in an on-line tool or other declaration.

SECTION 8. DISCLOSURE OF OTHER DIGITAL ASSETS OF DECEASED USER.

Unless otherwise prohibited by the User or a court, a Custodian shall disclose a “catalogue of electronic communications” sent/received by the user and “digital assets, other than the content of electronic communications, of the user, if the representative gives the custodian:”

- 1) Written request
- 2) Certified copy of death certificate
- 3) Legal Docs (court order, letter of appointment, etc.)
- 4) Custodian may request:
 - a. Account Number (or other identifier)

²² 18 U.S.C. Section 2702 (b)(1) and (b)(3).

²³ UFADAA, p15.

²⁴ UFADAA, pp 13-16

²⁵ 18 USC Code Sec. 2701 - Unlawful Access to Stored Communications

- b. Evidence to link user to the account
- c. An affidavit that disclosure is reasonably necessary for administration of the Estate;
or,
- d. Court finding
 - i. That User had an account identifiable per a above or,
 - ii. Disclosure is reasonably necessary for administration of the Estate

Note: Section 7 relates to the Content of the Electronic Communication made by a decedent. Content refers to the actual writings within an electronic communication. This would include the content of emails sent or received by the User.

Section 8 relates to all other Digital Assets and also provides that a catalogue of electronic communications of the User may be requested by the Fiduciary.

POA: The Standards for Differing Fiduciary Roles are set out and are different.

- **POA's look for specific rights of disclosure but still makes disclosure uncertain.**

Powers of Attorney (Sections 9-10)²⁶

Section 9: DISCLOSURE OF THE CONTENT OF ELECTRONIC COMMUNICATIONS OF PRINCIPAL. If POA explicitly provides, then Agent may request that the content of Electronic Communications of Principal be disclosed. The Agent must provide certain information to the Custodian.

Section 10: DISCLOSURE OF OTHER DIGITAL ASSETS OF PRINCIPAL

IF POA provides general authority to act on behalf of a principal or specific authority over Digital Assets, the Custodian will provide a "catalogue" of electronic communications to the Agent or Digital Assets. Note: this does not include the actual content of electronic communications but does include other Digital Assets that are NOT electronic communications.

Trusts:

If Trustee is the Grantor/Settlor. Can provide that a Digital Asset be disclosed.

However, if the Trustee is not the Grantor/Settlor, there may be restrictions.

- o **Content: Must be clear consent to disclosure of content**
- o **Non-Content: No specific consent to disclose is needed.**

TRUSTS (UFADAA Sections 11-13)²⁷

SECTION 11. DISCLOSURE OF DIGITAL ASSETS HELD IN TRUST WHEN TRUSTEE IS ORIGINAL USER.

Custodian shall disclose to that trustee any Digital Asset held in the trust including a catalogue and content of electronic communications.

SECTION 12. DISCLOSURE OF CONTENTS OF ELECTRONIC COMMUNICATIONS HELD IN TRUST WHEN TRUSTEE NOT ORIGINAL USER.

²⁶ UFADAA, pp 17-19

²⁷ UFADAA, pp 19-22

Unless otherwise ordered by court, directed by the User, or provided in a trust, a Custodian shall disclose to that trustee the content of an electronic communication sent or received by an original or successor user and carried, maintained, processed, received, or stored by the Custodian in the account of the trust, if:

- 1) Written request
- 2) Certified copy of trust agreement (including direct consent to disclosure of content)
- 3) Trustee certification
- 4) Custodian may request that Trustee provide:
 - a. A number, user name, address (or other unique identifier) or
 - b. Evidence to link user to the trust

SECTION 13.²⁸ DISCLOSURE OF OTHER DIGITAL ASSETS HELD IN TRUST WHEN TRUSTEE NOT ORIGINAL USER.

Unless otherwise ordered by the court, directed by the user, or provided in a trust, a Custodian shall disclose a catalogue of electronic communications sent or received by an original or successor user and stored, carried or maintained by the Custodian in an account of the trust and any Digital Assets, other than electronic communications, in which the trust has a right or interest, if:

- 1) Written request
- 2) Certified copy of trust agreement
- 3) Trustee certification
- 4) Custodian may request that Trustee provide:
 - a. A number, user name, address (or other unique identifier) or
 - b. Evidence to link user to the trust

Guardians/Conservators:

Note: Conservators cannot access Content. However, with a Court Order, the Conservator can access a catalogue.

GUARDIAN/ CONSERVATOR (UFADAA SECTION 14)²⁹

SECTION 14. DISCLOSURE OF DIGITAL ASSETS TO [CONSERVATOR] OF [PROTECTED PERSON].

- a. Court may, after hearing, grant Conservator/Guardian access to Digital Assets of the protected person
- b. Unless otherwise ordered by the Court or directed by the User, a Custodian shall disclose to the Conservator/Guardian a catalogue of electronic communications if Conservator gives Custodian:
 1. Written request
 2. Certified copy of Court Order (which give Conservator/Guardian authority over the Digital Assets of the protected person)
 3. A number, username, address (or other unique identifier) or
 4. Evidence to link user to the account of the protected person

²⁸ UFADAA, pp 21-22

²⁹ UFADAA, pp 22-23

Balancing the duties of Fiduciary and Custodian

- **Fiduciaries** have identical duties for Digital Assets as for tangible property.
 - Authority is based on Terms of Service, copyright and Online Tools
 - Critical: **May not impersonate the user**
 - But, if the Fiduciary is authorized (Authorized User),
 - 1) May access as though no Custodian/no service agreement.
 - 2) And, you are an authorized user, you are not subject to computer fraud
 - 3) If you have authority to tangible property which holds Digital Asset AND you are an authorized user, then you can access the Digital Assets.
 - Can request closure of account
 - o Custodian may disclose info in account if required to terminate the account.
- **Custodian** 60 day response. Otherwise, Fiduciary can go to court.
 - May require a court order
 - Order must be specific and show that compliance will not violate the provisions of the Voluntary Disclosure of Customer Communications or Records statute
 - Custodian is immune from liability for following this Act.

DUTIES OF FIDUCIARY, CUSTODIAN (Sections 15-16)³⁰

SECTION 15. Fiduciary Duty and Authority.

- a. Legal duties mirror those for tangible property
 1. Duty of care;
 2. Duty of loyalty;
 3. Duty of confidentiality.
- b. Fiduciary's authority with respect to a Digital Asset of a User:
 1. Subject to the applicable Terms of Service (except as otherwise provided in Section 4. [User Direction for Disclosure of Digital Assets] regarding User's grant of authority to the Fiduciary)
 2. Subject to copyright and other law³¹;
 3. Limited to the scope of the fiduciary's duties;
 4. May not be used to impersonate the user.
- c. A Fiduciary with authority over the property of a user has the right to access any Digital Asset in which the decedent had a right or interest if not held by a Custodian or if there is no terms of service agreement.
- d. A Fiduciary acting within their scope of duties is an authorized user for purposes of computer fraud/unauthorized computer access laws.
- e. A Fiduciary with authority over the tangible, personal property of user:
 1. Has the right to access the property and any Digital Asset stored therein; and
 2. Is an authorized user for computer fraud and unauthorized-computer-access laws.
- f. Custodian may disclose information in the account if required to terminate the account used to access Digital Assets
- g. Fiduciary of user may request termination of an account. Request must be in writing; and,
 1. If user is deceased, include a certified death certificate

³⁰ UFADAA, pp 23-28

³¹ Includes *Stored Communications Act (SCA)* aka Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. Section 2701. Unlawful access to stored communications

2. A copy of letter of appointment, court order, etc.
3. If requested by Custodian:
 - A. Account Number (or other identifier)
 - B. Evidence to link user to the account
 - C. Court finding that User had an account identifiable per A above.

SECTION 16³². Custodian Compliance and Immunity.

- a. Custodian is required to comply with a request from Fiduciary within 60 days. Fiduciary may go to court for an order if Custodian does not comply.
- b. If Court Order received, it must show that compliance will not violate the provisions of the Voluntary Disclosure of Customer Communications or Records statute.³³
- c. Custodian may notify user
- d. Custodian may deny a request if Custodian knows of a lawful means of access
- e. The act does not limit a Custodian's right to require a Court Order that
 1. Specifies account belongs to Protected Party
 2. Specifies consent from Protected Party
 3. Contains a finding required by law. Note: that does not include this Act.
- f. The Custodian is immune from liability for following this Act.

If the Custodian complies with the court order in good faith, they will have immunity.

Sections 17-21³⁴ relate to Uniform Application, coordination with other laws and other constructive items.

Summary:

Ultimately, the Fiduciary must understand that oversight of Digital Assets requires specific knowledge of the laws and an expertise regarding these assets.

Planning is a key component to successful recovery of digital assets, preservation of wealth represented by those assets and the protection of information that is otherwise private. The most important components are to clearly state the intention of the Client regarding access they desire to provide to beneficiaries, tying those wishes to the User interfaces with their digital providers, making passwords and access available and updating that information regularly.

As a dialogue point, Digital Assets may be found in these ways:

1. On Personal devices: As pictures, books and music on phones
2. In cloud-based or Off-site storage: On email, social media or other accounts and payment accounts like Paypal, Amazon Pay, etc.

Potentially valuable Digital Assets also exist in the form of: Cryptocurrency and NFTs.

- These assets provide some unique challenges. The challenge is in how you identify, access and protect these Digital Assets.

³² UFADAA, pp 28-30

³³ The Stored Communications Act, 18 U.S.C. Section 2702 - Voluntary Disclosure of Customer Communications or Records

³⁴ UFADAA, pp 30-31

- Greatest Risk: Access to Digital Assets can often die with the user or be lost with a forgotten private key or wallet.

For the Fiduciary, UFADAA must be coordinated with Privacy Statutes, that must be considered in connection with solid oversight guidance. For fiduciaries a critical tool for that guidance can be found for special/unique assets as set forth by the OCC.

Access to Digital Assets is covered under UFADAA. Thus, the path to overseeing these assets can be carefully navigated through the provisions of that Act and direction provided in the controlling fiduciary document as well as coordination within User Agreements and Online Tools.

Questions/Takeaways:

- Are you prepared to discuss/administer these assets?
- Can you collect these assets, sufficient to liquidate?
- Are there concerns about accepting certain types of Digital Assets?

If you are going to take in these assets:

- Be prepared to clearly identify them in advance.
- Create or Hire the Expertise
- Seek Legal Counsel to help understand and balance the risk
- Enhance Your System Capabilities
- Have Clear Risk Management

These Digital Assets are becoming a mainstream item and their volatility and risk of loss are huge issues for Planners and Fiduciaries. Be Prepared! You will have find these in an estate soon.

Disclosure

The material presented herein is of a general nature and does not constitute the provision by PNC of investment, legal, tax, or accounting advice to any person, or a recommendation to buy or sell any security or adopt any investment strategy. The information contained herein was obtained from sources deemed reliable. Such information is not guaranteed as to its accuracy, timeliness, or completeness by PNC. The information contained and the opinions expressed herein are subject to change without notice.

The PNC Financial Services Group, Inc. (“PNC”) which is a Member FDIC, uses the marketing names PNC Private BankSM, PNC Private Bank HawthornSM, and Hawthorn Institute for Family Success[®] to provide investment consulting and wealth management, fiduciary services, FDIC-insured banking products and services, and lending of funds to individual clients through PNC Bank, National Association (“PNC Bank”), which is a Member FDIC, and to provide specific fiduciary and agency services through PNC Delaware Trust Company or PNC Ohio Trust Company.

PNC also uses the marketing names PNC Institutional Asset Management[®] for the various discretionary and non-discretionary institutional investment, trustee, custody, consulting, and related services provided by PNC Bank, National Association (“PNC Bank”), which is a Member FDIC,

and investment management activities conducted by PNC Capital Advisors, LLC, an SEC-registered investment adviser and wholly-owned subsidiary of PNCBank.

“PNC,” “PNC Bank,” “PNC Institutional Asset Management,” “Hawthorn Institute for Family Success,” “PNC Gifting Portal,” and “Retirement 1-on-1” are registered marks, and “PNC Private Bank,” “PNC Private Bank Hawthorn,” “PNC Financial Wellness Achievement Center,” and “PNC OCIO Premier” are service marks, of The PNC Financial Services Group, Inc.

Investments: Not FDIC Insured. No Bank Guarantee. May Lose Value.

Insurance: Not FDIC Insured. No Bank or Federal Government Guarantee. Not a Deposit. May Lose Value.

©2023 The PNC Financial Services Group, Inc. All rights reserved.