PROGRAM MATERIALS
Program #3004
March 18, 2020

The Basics of Digital Asset Planning

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

KLEINBARD LLC

The Basics of Digital Asset Planning

By: Jennifer L. Zegel, Esq., LL.M.

jzegel@Kleinbard.com / 267.443.4126

Three Logan Square
1717 Arch Street, 5th Floor
Philadelphia, PA 19103
Kleinbard.com

BIG FIRM EXPERIENCE. SMALL FIRM ATTENTION.

Introduction to Digital Assets

- Critical component of any estate and business succession plan.
- Planning will only evolve as new laws, regulations, and technologies emerge.
- Requires analyzing and inventorying digital assets, accounts, and data owned.
- Not all digital assets are transferrable.
- Privacy, storage, and cybersecurity matters must also be considered.

Reasons to Plan for Digital Assets

1. Ensure wishes are followed with the management, transfer, and disposal of digital assets.
2. Identify and inventory assets to avoid unnecessary loss or delays.
3. Make the transfer and disposal of digital assets easier.
4. Safeguard against identity theft and cybercrimes.
5. Average person has over 100 online accounts based on a recent McAfee study.

Definition of Digital Assets

- Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) definitions:
    1. Digital Assets: an electronic record in which an individual has right or interest.
    2. Electronic: anything relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
- **<u>Not</u>** computers, smartphones, tablets, or hard drives.
- Digital assets are the information stored on devices or in accounts in the cloud or online.

Five Categories of Digital Assets

1. ***Electronic Documents***
2. ***Social Media Outlets***
3. ***Financial Assets***
4. ***Business Accounts***
5. ***Miscellaneous***

Laws Governing Digital Assets

1. **Electronic Communications Privacy Act/Stored Communications Act (SCA).**
2. **Computer Fraud and Abuse Act (CFAA).**
3. **Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)** – Version passed in most states; predecessor **Uniform Fiduciary Access to Digital Assets Act (UFADAA).**
4. **Terms of Service Agreements (TOSA): Agreement that controls relationship between user and custodian and/or service provider.**
   - **Prohibits password sharing.**
   - **Establishes policies and procedures over accounts/assets.**

Computer Fraud and Abuse Act

Computer Fraud and Abuse Act, 18 U.S.C. § 1030 – cannot access a government or financial institution computer or computer used in or affecting interstate or foreign commerce or communication without authorization or exceeding authorization (or attempt to do so) and obtain information in a financial record.

Stored Communications Act

- **Electronic Communications Privacy Act/Stored Communications Act,** 18 U.S.C. §§ 2701-2712 – Electronic communication service and remote computing service providers are prohibited from knowingly divulging contents of communication while in electronic storage.
- Criminal penalties for violations.
- Silent on fiduciary access.

Stored Communications Act Continued

Exceptions to Content Disclosure:

- May be divulged to an addressee or intended recipient of the communication.
- May be divulged with the lawful consent of the originator or addressee or intended recipient.
- May be divulged with the lawful consent of the subscriber/customer

- Silent on access by fiduciaries.

RUFADAA

Default rule under RUFADAA – a user must give explicit consent for a fiduciary to access digital assets of a user.

Hierarchy of access:

Online tool

Estate planning documents (Will, Power of Attorney, Trust)

TOSA

Definition of Online Tool under RUFADAA

"**Online tool**" means an electronic service provided by a custodian that allows the user, in an agreement distinct from the TOSA between the custodian and the user, to provide directions for the disclosure or nondisclosure of digital assets to a third person.

● ONLY controls access to digital assets if offered and used.

● Facebook, Google, and Twitter currently have online tools on their platforms.

RUFADAA

If deceased user consented to (or court directs) disclosure of content, the Custodian shall disclose to the Executor the content if the following is given:

* Written request for disclosure
* Certified copy of death certificate
* Certified copy of Letters Testamentary
* Unless direction is in an online tool, a copy of will or other record evidencing User's consent to disclosure.

Additional RUFADAA Notes

- Preserves custodian’s access to user’s digital assets.
- Fiduciary has duty of care/loyalty/confidentiality.
- Fiduciary may not impersonate a user.
- Custodian may grant full or limited access to digital assets.
- Custodians may ask for additional information.
- RUFADAA cannot control all digital assets – some cannot be transferred at death.

Additional Custodian Requests

- Custodian may request additional information before disclosure, such as:
  - Account number, username, address or other unique subscriber or account identifier assigned by Custodian to properly identify user's account.
- If disclosure ordered by Court, may request findings that:
  - (i) User had a specific account with the custodian through identifiable information; (ii) disclosure of content would not violate federal law; (iii) in the absence of online tool, that user consented to disclosure, or (iv) disclosure is reasonably necessary for the administration of the estate.

CASES

Ellsworth, File No. 2005-296, 651-DE Oakland County, Michigan Probate Court (2005) - Custodian refused father of deceased member of military access to son's emails describing military experience, citing TOSA and privacy, the Court ordered custodian to release contents.

Matter of Estate of Swezey, Surrogate's Court, New York, Case Number: 2017-2976/A - Apple required to disclose photos stored in decedent's Apple account as they were not electronic communications requiring consent for disclosure.

Matter of Serrano, Surrogate's Court, New York, 2017 NY Clip Op. 27200 [56 Misc. 3d 497], June 14, 2017 – Google required to disclose decedent's contacts and calendar information as they are not communications under Stored Communications Act. Petitioner's request for authority to require Google to disclose contents of decedent's email denied without prejudice to later application to the Court by petitioner, with notice to Google, establishing that disclosure of that information is reasonably necessary for the administration of the estate.

CASES CONTINUED

In re Facebook, Inc., 923 F. Supp. 2d 1204 (2012) - Custodian's motion to quash a subpoena seeking information by family concerning decedent's account was granted as the request violated Stored Communications Act; court lacked jurisdiction to address whether the family may consent so that custodian may disclose voluntarily, as so ruling would be an impermissible advisory opinion.

Ajemian v. Yahoo, 84 N.E. 3d 766 (Mass.2017), cert. denied, No. 17-1005, 2018 WL 489291 (U.S. Mar. 26, 2018) - Executor may provide lawful consent on decedent's behalf to release contents. Lower court had refused to enforce custodian's forum selection clause and TOSA against estate administrators who sought to access decedents emails; remand to lower court.

Key Elements of a Basic Digital Asset Plan

1. Inventory all digital assets, hardware, and software. Do **NOT** have passwords with the inventory lists.
2. Consider password management tools. Explore using online tools (if available). Generally, any 3rd party access designations should be cohesive with fiduciaries in an estate plan.
3. Include provisions in estate planning documents that authorize or limit a fiduciary's access to digital assets.
4. Incorporate provisions in governance documents for a business that address access to digital assets.

Key Elements of a Basic Digital Asset Plan

5. Establish a system to regularly back-up data.
6. Analyze technical capabilities of individuals or professionals tasked with administering these assets.
7. Decide where to store inventories and password information, and establish notification procedures to key individuals.
8. Evaluate the tax treatment of various digital assets and valuation methods.
9. Determine if advanced planning is required.

Drafting for Digital Assets

- A digital asset clause in Wills, Trusts, POAs, and even guardianship orders should:
  - Establish lawful consent for access under RUFADAA, SCA, and CFAA.
  - Address the disclosure of content and electronic communications to a fiduciary.
  - Define digital assets.
  - Designate ultimate recipients of digital assets.

Storage of Cryptocurrency Keys

1. Cryptocurrency requires using public and private keys.
2. Various ways to store keys:

    a. Hot storage: stored online (exchange, app, online wallet).

    b. Cold storage: stored off-line (memory stick, air-gapped computer or safe).

Estate of Matthew Mellon

- Early investor in cryptocurrency.
- Invested $2M in the XRP coin on the Ripple network, which is designed for banks as a payment settlement system.
- Hid private keys on nano sticks under alias names in safe deposit boxes.
- Died in April of 2018 with no known instructions to access an estimated $300M in crypto.
- Estate is being probated in Los Angeles, California.

Steps in Estate Administration

1. Locating Digital Assets.
2. Obtaining Custody of Digital Assets.
3. Inventorying and Consolidating Digital Assets.
4. Safeguarding Digital Assets and Digital Identity.
5. Valuing Digital Assets.
6. Disposing/Distributing Digital Assets.

1. Locating Digital Assets

- Look to a decedent's device/computer
  - A decedent's device/computer will contain a treasure trove of digital assets (but the executor may not be able to access the assets).
  - On a computer or device, the executor may only access locally stored assets and information. Beware of devices that automatically reach out to the internet to update.
- Look to other digital assets
  - Other digital assets (such as a username/password list) may give the executor a guide as to where to locate digital assets.
- Look for Written Lists of Accounts
  - The decedent may have kept a list of his/her accounts, usernames, and passwords. Beware of using the usernames and passwords to access accounts.

2. Obtaining Custody of Digital Assets

- UFADAA
  - Stand in the shoes of the decedent
- RUFADAA
  - Access
    - Online Tools
    - Lawful Consent in Will
    - Terms of Service Agreements
    - Content vs. Catalogue
- No-FADAA
  - Terms of Service Agreements

3. Inventorying and Consolidating Digital Assets

- Does the Terms of Service Agreement Permit Transfer?
- Forward E-mail Accounts.
- Consolidate Cryptocurrencies.
- Consolidate Storage of Photos, Music, and Videos .
- Stop Automatic Payments.

4. Safeguarding Digital Assets and Digital Identity

- Store Digital Assets Securely Accessible Only to the Executor.
- Back Up Data, Password Protect Date, Encrypt Data.
- Copy and Archive Data (if legal).
- Change Passwords.
- Protect Digital Identity.

5. Valuing Digital Assets

- Sentimental Value.
- Monetary Value.
- Consider Estate, gift, and income tax implications and reporting requirements.
  - Hire appraisers with knowledge of digital asset classes.
  - Engage CPA’s versed in required area.

6. Disposing/Distributing Digital Assets

- Does the Terms of Service Agreement permit transfer?
- Are the restrictions on transferability being complied?
- Are the assets automatically deleted? If not, close online accounts that contain personal information.

Thank you. Any Questions?

Jennifer L. Zegel, Esquire, LL.M.

Kleinbard LLC

Three Logan Square

1717 Arch Street, 5th Floor

Philadelphia, PA 19103

E: jzegel@Kleinbard.com

T: 267.443.4126

Co-host of the Digital Planning Podcast:

http://www.kleinbard.com/podcasts/