Ten Ways to Protect Your Client's Digital Assets

Betsy Ehrenberg, CEO, Legacy Concierge

Introduction

Digital records have a huge impact on law firms, wealth managers, private client advisors, institutional trustees, financial consultants and family offices comprising the trust and estate administration landscape. When digital assets are left scattered in the cloud, the estate's components and their asset value are subject to devaluation and disappearance.

Strictly speaking, digital assets are content that is stored in any electronic format. That could mean images, photos, videos, files containing text, spreadsheets or slide decks. New digital formats are constantly emerging therefore the definition of a digital asset is always expanding as well. Rather than a definitive list of file formats that qualify as a digital asset, digital assets can be any content, in any format, that is stored digitally and provides value to the company, user or consumer.

Trusts and estates increasingly are comprised of digital assets in the form of computer records that represent assets owned or managed by the individual, their estate managers, fiduciaries and trustees. Given this expanded definition of digital assets (beyond social media, emails, messages and calendars) the scale and scope of an estate management effort that secures and protects digital assets is an open-ended complex responsibility.

Historical Perspective Concerning Digital Assets

Attorneys and others involved in estate administration need a systematic approach to handling these assets during probate. Attorneys have been writing articles in their law journals about this problem since 2013, presenting papers at their local, national and international association meetings, experiencing identity theft against some estates they are administrating. The Federal Trade Commission (FTC) received over 320,000 reports concerning identity theft in 2017 whereby the fraudster assumed the identity of the decedent and systematically reduced the value of the estate. Nationwide, over 13% of deaths each year result in reported theft representing a loss of over $1B in assets in 2017.[1] During this same time period, billing policies increasingly transitioned from hourly rates to fee-based (percentage of the estate) or fixed fee schedules in their private client, trust and estate practices. More and more professional firms are steering away from hourly charges for trust and estate administration thereby necessitating more efficient ways to administer estates containing digital as well as tangible assets. What else is happening?

Estate planning laws clarify how estate trustees access digital assets of any estate. Data control is removed from the vendor and is restored back to the fiduciary. Having a list of sites before passing is optimal, but the laws provide processes by which fiduciaries can gain access when that is not available. When the user consents or the Court orders, estate administrators can access the content of the electronic accounts.[2]

Legislation – Fiduciary Access to Digital Assets

Digital asset access legislation in 46 of the 50 states and the District of Columbia include a section that reads, "The fiduciary cannot impersonate the user."[3] There are two devastating possibilities if a fiduciary (attorney or family member) impersonates the user to gain access to the digital assets, (banking records, investment securities reports, business ownership lists, real property deeds, PayPal transactions, airline miles, email, contacts, videos, photos and the like).

- If the fiduciary was an attorney, the result could potentially be disbarment;
- If the fiduciary was an heir, family member or beneficiary, then the administration process may move into litigation.

Impersonation typically happens while settling an estate holding a substantial inventory of digital as well as tangible assets, and when one of heirs or beneficiaries needs to take the custodian to court for refusing to release the asset (Ajemian v. Yahoo! 2017).

Practice Growth and Problem Growth

Attorneys and their clients increasingly acknowledge that trusts and estates contain electronic documents, logon credentials, digital assets, and may even include cryptocurrency, which since 2013, has become a very valuable digital asset; most savvy clients desire to work with an attorney who understands digital assets and acknowledges their value.[4]

Estates no longer consist of only financial accounts, real property, business interests and personal valuables. Asset documents do not solely reach the user by mail; one cannot sort through one's mailbox to locate all documents that represent a Client's assets.

Mailboxes still contain letters addressed to the decedent but they are often requesting donations, reporting non-profit growth, announcing university capital campaigns, soliciting political party support, and the like. It is practical to collect these mail items in order to stop delivery; after collating the mail, the fiduciary should contact the sender initiating another level of privacy for the family.

Estate planning should include discussions about the disposition of digital assets such as social media, email history, intentionally-hidden investments, contact lists, and shopping history. These assets will need resolution post-death. Plans should include instructions for emails, contact groups, personal websites, membership lists, manuscripts, video libraries, musical play lists, photo and patent royalties and electronic billing. Electronic billing includes memberships, subscriptions, magazines, news delivery, research providers, medical appointments, power utilities and household services such as security, gardener, snow removal, cleaners, home-care, and the like.

Ten Ways to Protect Your Client's Digital Assets – Protect Your Own Digital Assets

Organize and document digital assets by storing asset descriptions in a secure and private electronic location, and providing a roadmap to access digital asset disposition instructions after death. One's legacy should live on forever, their accounts should not.

1. Everything is digital. Identify digital assets, or electronic records of all digital and tangible assets that someone would be interested in or have a right to. When paper records exist, create digital versions of these documents in order to create an electronic record; create a summary of where those paper records are filed. At some future time, you can review those paper records, the locator, and decide to digitize their contents and secure them in an electronic location (on your computer or on a flash drive or both). Some individuals still do not trust electronic storage even though they 'should'.

2. Assets are at stake. Identify client's personal accounts at banks, brokerage firms, investment and retirement companies as well as your client's trust accounts and their supporting documents. Past tax returns with K-1 and Schedule C sections are the tea leaves to successful searches. It is remarkably easy to impersonate the decedent using an automated Internal Revenue System (IRS) answering service in order to obtain previous years' tax returns. It is also against the law to impersonate the user at any time.

   Digital asset and electronic record information is sprinkled throughout tax returns; your Client can obtain copies of returns on an annual basis to aid in protecting their digital assets and preserve the value of their estate.

3. Document your Client's wealth and estate components. Digital assets include the electronic records that describe the wealth and estate. Wills and trust documents should clearly include a definition of 'digital assets' and specify the 'digital executor,' the person who is responsible for those assets during probate. By cataloging the digital asset components, your Client is acknowledging their value and recognizes the need to have a plan for handling those assets.

   User credentials to access digital assets are needed when the person is living; these credentials have greater value when the user has passed. Smart phones and tablets often contain valuable digital asset descriptors. Document how to access the contents of smart-phones and tablets in order to process the following data collections:

   a. Calendar. What events are scheduled for the current month? Is there a calendar with contacts' birthdays? Does anyone care about the calendar history? Are there any future appointments needing cancelation?

   b. Voicemail. What user credential is needed to listen to saved messages and view frequently contacted persons?

c. Contact lists. Who should be notified and who should not? Are there any group designations and are they current? When was the last time the client looked at the directory and its groups?

d. Photo gallery. Is the gallery organized? What is in each gallery group - pictures, albums, stories, and/or shared? Where should these photos be archived? Is there an urgency to move photos to another device? Who should have custody of these images?

e. Messaging. Are there scheduled messages? What should happen to the photos and videos? Who should be notified from the messaging contact list? What should happen with the links, audio and glimpses, emergency contacts and ICE directives.

f. Review the applications uploaded on phones and tablets in order to locate subscription services and social media forums that need to be contacted. Popular sites include the following:

   i. Ride-sharing (Lyft, Uber)
   ii. Shopping (Amazon, eBay, Costco, Yelp, Play Store)
   iii. News (CNN, YouTube, Prime Video)
   iv. Social (Facebook, LinkedIn, Instagram, Twitter, Whova)
   v. Financial (Banks, Brokerage, Plastic Cards, Theft Protection)
   vi. Airlines (Southwest, American, United, Delta)
   vii. Hotels (Starwood, Marriott, AirBnB, VRBO

4. Secure all electronic accounts. While the person is living, each of their digital accounts should have two-factor authentication or better. Passwords should be changed regularly; password changes often are initiated by the custodian (social security administration, state departments) because certain financial and government agencies recognize the user name, but demand for security purposes that the user change their password before clearance.

   More and more websites and services use two-step or two-factor authentication to provide an additional layer of security. This security technique verifies your identity when you log into a website by requiring you to both *know something* and *have something.*

5. Escheated or abandoned property is held by government departments in each state. The first enactment of unclaimed property laws appeared in 1954 and Revised Uniform Unclaimed Property Act was passed in 2016. In most states, online portals are available for searching for escheated or abandoned property on behalf of decedents and your Clients. While most accounts hold less than $100 for any individual, there are certain cases where the escheated property is worth thousands of dollars.

Many Secretaries of States taxing departments user the services of an outside firm (missingmoney.com) for indexing all abandoned property. For more information about abandoned or escheated property, visit the National Association of Unclaimed Property Administrator (NAUPA) at unclaimed.org.

6. Subscription cancelation is not only economically justified but reduces angst for the fiduciary, heirs and companies providing subscription services. Organizations often sell their subscription databases, therefore removing the decedent's name, and may want to reduce unwanted communication in the future due to communications and marketing costs.

   Credit card statements include subscription payments; bank account statements indicate ACH payments. Use this information to stop subscriptions.

   When possible, obtain statements for the previous December and January for annual payments. If possible, access statements for twelve months to locate all subscription payment activity.

   a. Magazine labels include the subscription expiration date; since publishers do not want to lose subscribers and advertisers, they will often continue mailing periodicals even if the annual fee is not paid.

   b. Wine club annual fees are often charged to a registered credit card. When you want the shipments to stop, contact the company and demand that they update their subscriber files and discontinue service.

   c. Country club, tennis and golf club memberships often bill monthly, quarterly or annually. Once membership fees have been identified on bank and credit card statements and membership is no longer viable, it is time to stop membership newsletters and contact the administrator requesting that they update their organization's files.

   d. Professional membership organizations and university alumni offices often receive annual donations from the decedent. These payments appear on credit card and bank account statements; follow-up is done through email and donation requests. Cancellation contact information is prominently displayed on the solicitation.

7. Collections may be extremely well-organized with bills of sale, provenance records, artist statements, photos and current appraisals. Art, jewelry, wine, furniture, stamps, coins and other collection documentation are part of an estate and take the form of electronic records. Hopefully collection contents are indexed and stored electronically using one of many online applications.

8. Digital assets of significant value reside in a variety of hidden locations, but that does not diminish their significance nor provide any excuse for not including them in your discussions and proposed trust and estate administration plan. In order for the fiduciary to discharge its duties "with the care, skill, prudence, and diligence under the circumstances then prevailing," the attorney can use a variety of application portals to collect digital asset information.[5]

   Online portals provided by the US Patent and Trademark Office support search for patents ownerships. Royalty income may appear on tax returns; non-royalty intellectual property belonging to the estate may be significant but not currently generating income. Inventor search is available online and the inventor name must be formatted in a specific way; instructions are available and published in "How to Search for Patents by Investor."[6]

   Manuscripts by researchers and professors, published and unpublished, ready for editor review often reside on the decedent's computer. For additional security and backup reasons, many authors use Google's Doc services to store their creative materials.

   "Android tablets and phones come with limited storage space when compared to PCs, and so using some form of external storage is essential. All tablets and phones can be configured to use cloud storage like Google Drive. There are many cloud storage providers, and most provide a free limited storage allowance which can easily be expanded as required. All Google accounts come with a free 15GB allowance on Google drive."[7]

   Travel journals, photo albums and video clips are part of one's digital inventory. These digital assets constitute memorabilia that can be catalogued during trust and estate planning.

9. Social groups and membership rosters, one's social life, is digital and expansive. Names, addresses, emails and phone numbers may reside with many public and private organizations. Imagine the embarrassment by the membership chair when they solicit donations, nominations, dues and contributions of a deceased person!

   Often the membership chair, donor retention manager and newsletter editor are not notified of an individual member's death. Social groups' digital assets may include the name of the decedent for years unless the fiduciary provides notification of the death and verifies that the decedent's name has been removed from the organization's files.

   Deactivating the decedent's email address may not protect the digital asset that is maintained by social groups. Social club leadership may be expecting timely reports and/or meeting attendance from the decedent. To reduce embarrassment, disappointment, and expense, it is vital and appropriate to provide formal notification to each social group for their record keeping and the decedent's privacy.

10. Social media accounts are populated all over the internet. Even if the decedent did not plan to be on social media, their photos and vacation activities may be presented with a search engine. Getting the decedent's information removed not only protects the identity but provides emotional comfort to successors. If you want to test this out, do a search on a person you know has passed and count the number of times their name and image displays.

Summary and End Notes

Protecting the estate and its digital assets is an ongoing activity. Knowing where to start, what information to collect and keeping on top of the process is a monumental task. If left to the successor and/or the fiduciary, many digital assets and electronic records will remain in cyberspace potentially creating accounting and disposition resolution problems that are costly and embarrassing.

Digital assets represent and are a dynamic road map to major portions of an estate. For this reason, attorneys and wealth managers, trustees and financial planners have a compelling reason to conduct an annual digital asset review with their Client. Although a secure digital asset library may have been built at the beginning of the Client's trust and estate planning process, content review and updates should be done periodically.

One's legacy should live on forever, their accounts should not.

End Notes

1. "Identity Theft Statistics", ftc.gov/idtheft, 2017 data reported in 2018
2. "Understanding Uniform Fiduciary Access to Digital Assets", Jeff Perkins, June 2017
3. "Revised Uniform Fiduciary Access to Digital Assets Act", NM SB60, January 2018
4. "IBM Reports on Cryptocurrency", money.usnews.com, May 15, 2013
5. "The Mac Security Blog", Kirk McElheran, March 2016
6. "How to Search for Patents by Inventor", Mary Bellis, March 2018
7. "The Digital Fiduciary", Shlomo Benartzi, March 2019