BNY MELLON
WEALTH MANAGEMENT

Planning for and Protecting Your Digital Assets

In our increasingly digital world, the average person is reported to have over 25 discrete online logins, a number that is probably vastly understated, especially for wealthy investors. In addition, e-commerce businesses, valuable domain names and revenue-producing blogs — to name just a few — are an increasing source of wealth. Yet many individuals don't fully comprehend the breadth and complexity of the assets and information they hold online.

As a result, many people are not adequately protecting their assets during their lifetimes, let alone planning for their effective administration, protection or ultimate transfer after death or incapacity. Moreover, because the online world is a relatively new phenomenon, current law is rapidly changing in order to address the realities of digital asset management and disposition. Individuals need to be continually tracking their digital assets and reviewing their estate plans to ensure they are aligned with their wishes and current laws.

Defining Digital Assets

One of the first challenges in navigating the complex web of digital assets is completely defining what digital assets are. The definition is constantly changing and can also be subject to differing interpretations. Generally speaking, they include:

- Electronic data that may be stored on a computer, phone, tablet, external hard drive or other device, or remotely in the cloud (e.g., photos, videos, songs, computer programs, documents created using Microsoft Word or Excel, etc.)
- User accounts that allow people to access a tangible device, access to services or data on an online service, typically with a unique username and password (e.g., computer, phone, tablet, email, social media accounts, banking, brokerage or investment accounts, music, photo or video services, gaming and entertainment, e-commerce sites, etc.)
- Virtual or digital currency that represents some measurement of value and has a medium of exchange or transferable value (e.g., Bitcoin, Litecoin, Ethereum, online gaming currencies, airline frequent flyer miles, credit card rewards, personal digital records, etc.)
- Domain names that you use for a personal business or blog or own for other reasons, such as for future use or investment purposes
- Intellectual property rights such as copyrights, trademarks and patents that are tied to digital assets

Digital Asset Risks

Digital assets permeate all aspects of our lives, so it is important to understand the issues they can present for the original owner, his or her heirs, and the representatives and fiduciaries assigned to the assets' stewardship or disposition.

Inventory of Accounts and Cybersecurity

Three main issues that owners of digital assets and their fiduciaries face are:

1. Identifying all of an individual's digital assets
2. Providing fiduciaries access to these assets after the individual dies or is incapacitated
3. Protecting against cybersecurity threats both during life and after death or incapacitation

Balancing these can be extremely difficult. Given the complexity of most people's digital lives, it can be nearly impossible to completely and correctly identify all digital assets without the owner's very thorough organization and communication in advance. Even if all digital assets are accounted for, the next challenge becomes providing the information needed to access them. While passwords and encryption services are essential to protecting digital assets, they are also the main obstacle for a fiduciary or loved one attempting to access them.

Shifting and Conflicting Law

Current law is also a major challenge — much more so than for non-digital assets. A plethora of regulation and controls at multiple levels — federal, state and service providers — endeavor to protect individual privacy and the security of online assets. Unfortunately, many of these laws exist to protect digital assets from being accessed by anyone other than the asset owner, and the laws that exist to help facilitate access by other users are fluid, murky and sometimes conflicting due to the relatively new terrain the digital world has created. In many cases, even with appropriate authorization and instruction, a well-meaning fiduciary could be liable for criminal action simply for accessing a decedent's online records.

Exhibit 1

What Is Digital?

While the definition of digital assets continues to evolve and can include an endless litany of items, some common types include:

CDs, DVDs, thumb drives and cloud storage	*Dropbox, iCloud, Google Drive*
Email accounts, passwords and history	*Microsoft Outlook, Gmail, Yahoo! Mail*
Online financial services, including banking, purchasing and bill-paying services	*Online banking, investment and brokerage accounts, PayPal, Venmo, Google Wallet, Square Cash*
Loyalty program benefits, including credit card reward and airline or hotel points	*Many programs are eligible for gifting to charity*
E-commerce websites	*eBay, Craigslist, Amazon, Etsy, Alibaba, Walmart.com, Zappos*
User names and passwords on devices, servers, software or online apps	*Tablets, PCs, phones*
Photos, scrapbooks, music, videos, iTunes accounts and voice records	*Copyrights, trademarks or patents may be tied to these assets*
Social media accounts and profiles	*Facebook, Snapchat, Instagram, Twitter, Slack*
Ventures, businesses and other assets that only exist digitally	*Social media ventures, online business, domain names, digital and virtual currencies and websites*
Password-protected/encrypted documents	

In an effort to address this problem, the Uniform Law Commission[1] approved the Uniform Fiduciary Access to Digital Assets Act (UFADAA) in the summer of 2014. This act would have given fiduciaries (including personal representatives/executors, agents for power of attorney, conservators for protected persons/individuals and trustees) the authority to access digital assets in a manner similar to how they access other tangible assets, such as a house, car or artwork. It would have also minimized liability, which fiduciaries otherwise are exposed to given existing federal and state privacy and computer-hacking laws. However, Delaware was the only state to adopt it. In other states, lobbyists were able to defeat it.

Recognizing defeat, the Uniform Law Commission approved a Revised Uniform Fiduciary Access to Digital Assets Act (Revised UFADAA) in the summer of 2015. As of early 2017, 32 states had enacted a version of the Revised UFADAA and another 11 are considering it.

Important Terms

The first term is "service provider," sometimes referred to as "custodian." These are the companies that store the digital assets or information (e.g., Google, Amazon, Apple, etc.). Most service providers have a terms of service agreement (ToS) that govern the relationship between the service provider and the user. They are the stated legal policies as to how the service provider handles and protects its clients' information that users must agree to and abide by in order to use the service provider's services or website. Most of us, when faced with a service provider's online ToS, blithely click "accept" without reading the fine print. Yet the specific provisions in each of these agreements may actually block access — or even ultimate ownership — for heirs and administrators.

The other terms to understand relate to the types of information that service providers have that fiduciaries will want access to or control of after the user is gone or incapacitated. The first is a "catalogue" of electronic communication. This is merely the information of the user, the date and time the communication was accessed or created and the person to whom that communication was sent to or received.

Think of it as the information that goes on the outside of an envelope for a traditional piece of mail. The content inside the envelope, the actual letter, is the "content" of electronic communication, both sent and received by the user. While these relate to types of communication, not all digital assets are catalogues or contents. Other assets are typically defined by the general term of "digital assets."

Determining Who Has Access

Prior to Revised UFADAA, many service providers refused to provide fiduciaries or families access to any digital assets of a decedent based on either federal data communications laws or the service provider's ToS. Not all terms of service addressed what happens to a user's account or information at death or incapacity, but some did. One of the more infamous is Yahoo's ToS, which states that a user's account rights terminate upon death, theoretically prohibiting access by any parties subsequently. Yet some, like Facebook and Google, allow users the ability to pass on caretaking of their profiles or accounts after their death or to elect to have their accounts terminated. As with all things digital, it is important to note that the pace of change in this area is incredibly rapid.

Under Revised UFADAA, if a service provider provides an online tool similar to Facebook's "Legacy Contacts" or Google's "Inactive Account Manager" that allows the user to make an election granting another person access to the account or content or to terminate the account, the account user's instructions under that action trump all other instructions. If a service provider does not provide for an election separate from its normal ToS or the user elects not to use that option, then the user's instructions contained in a will, trust, power of attorney or other written record will be enforceable. If the user has failed to do either of these options, then the service provider's ToS will determine access. If the ToS does not address this issue, then default state law under Revised UFADAA controls.

But what if the state has not enacted a version of Revised UFADAA? Then the fiduciary's options are more limited. The fiduciary may request the service provider for access, and if that is not granted, file a civil lawsuit against the service provider. The success rate under this last option is extremely mixed.

How to Access

Under the default rules of Revised UFADAA, a fiduciary named in a will, trust, power of attorney or other document may request access to a catalogue of electronic communications and other digital assets in the same manner a fiduciary would request access to other tangible assets. This power is implied in the naming of that fiduciary. To prohibit a fiduciary from accessing a catalogue of electronic communications and other digital assets, the user would have to specifically state the limitations the user wished to place on access to these types of assets in the document that names the fiduciary.

[1] The Uniform Law Commission is a group of practicing lawyers, judges, legislators and legislative staff and law professors who have been appointed by state governments as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands to research, draft and promote enactment of uniform state laws in areas of state law where uniformity is desirable and practical.

To access the contents of electronic communications, the user must specifically consent to the disclosure in a will, trust, power of attorney or other document. Simply naming a fiduciary in those documents is not sufficient. If the user does not proactively plan for this access by specifically addressing it prior to death or becoming incapacitated, it may be extremely difficult, costly or impossible for a fiduciary to receive access to or control of the contents.

Additionally, it is important to understand that this area of law and the Revised UFADAA are in its infancy, and so it is not entirely clear how all companies will handle requests from fiduciaries or other named parties, or how courts will interpret these powers, requests and disagreements between fiduciary and service provider.

The Risks of Not Planning

Failing to plan ahead for the ultimate disposition of digital assets not only creates more work for a fiduciary, but also increases the risk of the fiduciary not gaining access to them. It also increases these other risks:

- **Missing items**. Without a list of all digital assets, a fiduciary may never locate or discover all of the existing digital assets.
- **Identity theft**. The longer it takes a fiduciary to gain access to digital assets, the longer it may take to uncover any fraudulent activity. Additionally, potential criminals are known to prey on the assets of the deceased. About 800,000 deceased Americans' identities are deliberately targeted for misuse annually (2.4 million deceased identities are used improperly in total each year).[2]
- **Asset erosion**. The damaging effects of time can be a particular problem for digital assets. Imagine how quickly the value of an online business can erode if that business has to be left untended while an estate's personal representatives and heirs try to prove their rights to access and manage the business or locate the digital keys to do so.
- **Unwanted access**. Often, it is just as important to think about what should not be made available or passed on. Personal emails and documents can cause immeasurable harm to family members at the worst possible time when private issues, family secrets or other confidential comments are inadvertently left behind.

Given all of these risks, wills and other publicly accessible documents are not appropriate communication vehicles for sharing digital asset information. Even a simple paper document or electronic file left with a trusted party can present risks. Encrypted files, online storage accounts or other accommodations are options, but each has benefits and disadvantages that should be evaluated and discussed with knowledgeable experts.

Preparing and Protecting Your Digital Assets

Digital assets and the laws governing access to them at death or incapacity are constantly evolving. While not all states have enacted a version of Revised UFADAA, it has quickly spread across the country and has been implemented or is under consideration in two-thirds of U.S. states as of early 2017.

The widespread implementation of these laws is encouraging for all parties involved. However, the inconsistency and uncertainty from state to state can make it difficult for individuals to effectively plan for the treatment of their digital assets. To confront this challenge, it can be helpful to follow these simple rules:

- **Create an inventory**. Look beyond the obvious as you catalogue your financial accounts and passwords: personal digital records and mementos (e.g., emails, social media, videos, photos, voice recordings, etc.); passwords and guidelines for accessing all personal devices and password-protected documents; business and enterprise assets and more. Options as to where and how to store this inventory may vary. For instance, online resources (e.g., Secure Safe, Legacy Locker and Asset Lock) are available, but some may prefer the old fashion safe deposit box or leaving with a trusted advisor. Whatever your preference is, be sure to consult with your legal advisor as to which solutions may be appropriate for you.
- **Inspect service-provider-specific tools and ToS**. Research whether a service provider has an online naming and instruction tool and decide whether you want to use it. If it doesn't, read the service provider's ToS to determine whether it provides for rules and regulations that may assist your fiduciary or that could impede your designees' ability to lawfully execute their duties.
- **Update your estate plan to provide clear authorization for access**. This is particularly important. Explicit written permission as to your fiduciary's authority to access (or not access) your digital assets should be made in your estate-planning documents (i.e., will, trust or power of attorney) or in a separate written document. Even a simple paper document or electronic file left with a trusted party can present risks. Encrypted files, online storage accounts or other accommodations are options, but each has benefits and disadvantages that should be evaluated and discussed with knowledgeable experts.
- **Draft clear and secure instructions and documentation**. These instructions should include how to access, administer, transfer and even potentially destroy records. However, detailed instructions or private information should not be disclosed in a will or other public document.
- **Get expert legal advice**. Given the fluidity and complexity of digital law, this is critical.

[2] ID Analytics' ID: A Labs, April 2012.

– **Revisit and update your information regularly**. Documentation should be updated whenever a new account or digital asset is acquired, but this also may be needed as technology advances, a service provider's ToS changes, state or federal legislation evolves or family dynamics warrant.

– **Stay informed (or ensure that your advisors do)**. The protection of digital assets is one of the fastest changing and most complex areas of wealth-planning and protection today. Staying on top of this change and how it could impact you or your heirs is of paramount importance. Many resources are available to stay informed (e.g., deathanddigitallegacy.com, *Your Digital Afterlife* by John Romano, thedigitalbeyond.com, digitalpassing.com).

Awareness, preparation and expert guidance are some of the most powerful tools available to help you protect your online wealth. The time and thought you invest in doing so will be invaluable, especially given that digital assets are sure to be an increasingly significant portion of your wealth in the future.