Digital Wealth

PLANNING FOR AND PROTECTING A GROWING SHARE OF YOUR PERSONAL NET WORTH

BNY MELLON
WEALTH MANAGEMENT

As we all know, the world we live in is increasingly digital. The average individual is reported to have 25 passwords, a number that is probably vastly understated, especially for wealthy investors. In addition, electronic commerce—online businesses, valuable domain names, and revenue-producing blogs, to name just a few—is an increasing source of livelihood and 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 does not adequately address the realities of digital asset management or disposition.

Defining Digital Wealth

One of the first challenges in navigating this complex issue is completely defining what digital assets are. Generally speaking, they can include:

- an asset with tangible value, that only exists digitally (an online store, for instance, or digital currencies such as Bitcoin);
- electronic records and devices that provide access to other assets (e.g., online brokerage or investment account assets) or debts (PayPal or other bill payment accounts); and
- personal digital records that may have no transactional value but have an immeasurable value to oneself or one's family and friends (e.g., photos, social media accounts, music, voice recordings, email messages, personal documents, etc.).

Exhibit 1 provides some examples of these important assets, to give a sense of their range. However, like technology, the definition of digital assets is constantly changing and can also be subject to differing interpretations. Any list essentially would have to be constantly expanded and updated in order to cover every possibility.

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;
• Email accounts, passwords and history;
• Financial assets accessible online, including account information and passwords;
• Loyalty program benefits, including credit card reward, and airline or hotel points (many programs are eligible for gifting to charity);
• Online sales, purchase or bill-paying accounts and records (e.g., PayPal, Ebay, etc.);
• Online storage accounts;
• Passwords on devices (e.g., tablets, PCs, phones), servers, software or online apps;
• Password-protected/encrypted documents;
• Photos, scrapbooks, music, videos, iTunes accounts, and voice records;
• Social media accounts and profiles; and
• Ventures, businesses and other assets that only exist digitally (e.g., social media ventures, online business, domain names, digital currencies and web sites).

Digital Asset Risk

In thinking about digital assets, it is important to understand the problems they can present for the original owner, his or her heirs, and the representatives and fiduciaries assigned to the assets' stewardship or disposition.

Inventory Issues

Perhaps the most obvious problem is the challenge of capturing and accessing all associated assets and records. Given the complexity of most people's digital lives, it can be nearly impossible to completely identify all information and assets correctly or secure their access and protection without the owner's very thorough organization and communication in advance.

Shifting and Conflicting Law

Current law also is a challenge. A plethora of regulation and control at multiple levels—federal, state and even service provider—endeavors to protect individual privacy and security of online assets. Unfortunately, due to the relatively new terrain the digital world has created, these laws are fluid, murky and sometimes conflicting. In many cases, even with appropriate authorization and instruction, a well-meaning personal fiduciary could be liable to criminal action simply for accessing a decedent's online records.

In an effort to address this problem, the Uniform Law Commission approved the Uniform Fiduciary Access to Digital Assets Act (UFADAA) in the summer of 2014. This Act goes a long way toward clarifying fiduciaries' (including personal representatives/executors; agents for power of attorney; conservators for protected persons/individuals; and trustees) authority to access digital assets. It may help to resolve the liability to which fiduciaries otherwise are exposed, given existing federal and state privacy and computer hacking laws. However, how, where and when this Act is adopted is in the hands of state legislatures, for their particular jurisdictions. As of January 1, 2015, only Delaware had adopted it, although other states have it under review.

In the meantime, states continue to grapple with the complexity of digital asset administration, including for non-fiduciaries. Five states, for instance, have so far passed "next-of-kin laws" that try to help deal with the challenges of digital assets after death and during incapacity (i.e., Indiana, Rhode Island, Connecticut, Idaho and Oklahoma), and virtually all other states have this on their radar. Nebraska was the latest to introduce legislation, and others surely will follow.

An often overlooked legal issue is service-provider-specific rules. Each provider has stated policies as to how it handles and protects its clients' information, and in some cases these policies could overturn the best-laid plans formed either by you, your advisors, or even existing legislation. Most of us, for instance, when faced with a service provider's online Terms of Service Agreement ("TOSA"), 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 obvious TOSAs people think about are financial in nature, but it is important to note that this potential problem exists for any online service. A simple and often-cited example is Yahoo's TOSA, which states that a user's account rights terminate upon death, thus in theory prohibiting access by any parties subsequently. As with all things digital, it is important to note that the pace of change in this area is incredibly rapid. For instance, Facebook recently introduced "Legacy Contacts" to give its account holders the ability to pass on caretaking of their profiles after their death. Other online providers continue to evaluate and update their approaches to handling this issue as well, making staying on top of current rules an ongoing challenge.

Control and Confidentiality

Security and privacy also are concerns. While it is important to leave a trail and instructions for how to access information, protection of that record is just as critical. About 800,000 deceased Americans' identities are deliberately targeted for misuse annually (2.4 million deceased identities are used improperly in total each year, or 2000 daily)[1].

Given this risk, 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 both benefits and disadvantages that should be evaluated and discussed with knowledgeable experts.

In addition, it often is just as important to think about what should not be made available or passed on as what should. 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.

Asset Erosion

Lastly, 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.

Preparing and Protecting Your Digital Wealth

No plan is complete without thoughtfully accounting for digital assets. How to go about this is not always straightforward, given the pace of change and complexity of current regulations. However, following some simple rules of thumb can help. These include:

- **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, person to person. For instance, online resources (e.g., Secure Safe, Legacy Locker and Asset Lock) are available, but be sure to consult with your legal advisor as to which solutions may be appropriate for you.
- **Draft clear and secure instructions and documentation:** These instructions should include how to access, administer, transfer and even potentially destroy records.
- **Provide clear authorization for access:** Explicit written permission as to your designee's authority is important. Increasingly, language is being included in trust and other estate documents that explicitly authorizes trustees or other delegates to have access to, and control of, digital assets. Don't assume, however, that your saying so is always enough. Inspect service-provider-specific TOSAs and other rules or regulations that could impede your designees' ability to lawfully execute their duties.
- **Ensure your intentions for your digital assets are fully accounted for within your estate plan:** This is particularly important for assets that only exist online and have significant financial value (e.g., domain names, digital currencies, online businesses and blogs), as opposed to assets that are typically accessed online but are already accounted for within a will or trust document.
- **Get expert legal advice:** Given the fluidity and complexity of digital law, this is critical.
- **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, service provider TOSAs change, state or federal legislation evolves, or family dynamics warrant.

Implicit in this last recommendation, of course, is the need to stay informed, or to 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 (examples include: deathanddigitallegacy.com, "Your Digital Afterlife," by John Romano, and thedigitalbeyond.com), and your advisors also should be an important resource.

Especially with regard to the evolving world of digital assets, 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 this relatively new asset type is most likely an increasingly significant portion of your wealth.

[1] ID Analytics' ID: A Labs, April 2012