

# Protecting Digital Assets After Death\*

Nicholas J. Kaster  
*Fall 2016 Firm Newsletter*  
11.15.2016

One of the more challenging elements of estate administration is identifying the decedent's assets. In the past, family members or friends responsible for administering the estate were told to look through the decedent's file cabinets, watch the mail, and review old tax returns in order to find clues about the assets. Although not perfect, these strategies usually provided the needed information.

With the advancement of the Internet and e-based services and products, the tried-and-true strategies of asset location are becoming less reliable. More and more bank and credit card statements are being delivered via e-mail, bills are being paid by online services, funds are deposited in Internet-only banks, income tax returns are prepared online, and pictures are stored on phones and tablets. As a result, there are fewer documents stored in file cabinets or delivered via U.S. mail. The Internet has also created new marketplaces to purchase music, videos, and other content.

As a result of technological advances, a person's assets, in addition to real estate, bank, and investment accounts, may also include a PayPal account, a cache of Bitcoins, websites, and a blog.

Like tangible assets, "digital assets" may have monetary value and contain personal or private information that merits protection. However, unlike tangible property that is safeguarded using physical measures (e.g., safe deposit boxes, in-home safes, locked file cabinets), digital assets are protected through the use of biometrics, passwords, and usernames. Moreover, digital assets can be safeguarded at the hardware level to require a password to access the phone, tablet, or computer; and at the asset level to require a username and password to access an account, website, or software.

Reliance on passwords is an effective protection strategy because, in most cases, they are not shared with others or written down. When administering an estate, encountering password-protected hardware and digital assets can preclude the discovery of assets and potentially affect the amount received by beneficiaries, family members, or heirs.

Many people overlook the monetary and sentimental value of digital assets and the information needed to ensure they are discovered and administered according to their estate plan. The following are suggestions we encourage clients to think about for their digital assets:

## **1. Conduct a Digital Audit.**

Conduct a "digital audit" and create an inventory of various classes of digital assets (e.g., email accounts, social media accounts, hardware, and software). The inventory should list the username, account number (if applicable), and password for:

- Hardware (e.g., computers, mobile phones, netbooks, notebooks)
- E-mail accounts
- Social media accounts
- Blogs, domain names, and websites
- Photo accounts
- Financial accounts

## **2. Consider Options For Storing Username and Password Information.**

The most challenging aspect of creating a plan for digital assets is overcoming the justifiable fear of consolidating passwords, account numbers, and usernames in one document. Some prefer a handwritten list stored in a safe deposit box or some other secure location – while others favor an electronic list stored on an encrypted USB drive.

Considering the frequency with which passwords are changed, updating the digital inventory presents an additional challenge. Establishing two or more dates per year (e.g., children’s birthdays or daylight saving time) has proven to be an excellent reminder to review and update the inventory. Alternatively, a password managing service can be used.

## **3. Review and Update Estate Planning Documents.**

Review your wills, revocable trusts, and powers of attorney to ensure that these documents authorize an individual to access and manage digital assets. Minnesota recently adopted the Uniform Fiduciary Access to Digital Assets Act (UFADA), which allows personal representatives, trustees, attorneys-in-fact, and other authorized agents to manage digital assets. Because UFADA will allow a fiduciary access to e-mail, text messages, and social media accounts only if the fiduciary is specifically authorized to do so in writing, it is increasingly important to ensure that provisions addressing digital assets are included in estate planning documents.

## **4. Make a Plan for Managing Digital Assets After Death.**

Review the digital inventory and develop a written plan outlining how digital assets should be handled after death. In some cases, accounts may contain sensitive or secret information that is to be deleted and not revealed to certain persons.

## **5. Start Thinking About Your Digital Footprint.**

As digital assets become more prevalent in day-to-day life, they will also take on greater significance after death. Absent special efforts to help surviving family members and friends discover and access digital assets, individuals may be unintentionally sacrificing assets with significant emotional and monetary value. However, with a little forethought and planning, individuals can simplify estate administration and preserve these assets for their heirs.

*\*This article originally appeared in the June/July 2016 edition of Footnote, a publication of The Minnesota Society of Certified Public Accountants. Repurposed and republished with permission of the publisher.*

## **Attorneys**

Nicholas J. Kaster

## **Practice Areas**

Estate Planning and Wealth Preservation

