Federated Hermes

Digital Assets:
A guide to your digital footprint

Presented to

Presented by

Federated Securities Corp.
G85144-01 (11/24)

Before diving into digital assets, ask yourself…

- Do you have an email address?
- Do you belong to an airline or hotel rewards/loyalty program?
- Do you store digital photos on your phone or in a cloud-based platform?
- Do you use Facebook, LinkedIn, Snapchat, X (FKA Twitter) or Instagram?
- Do you pay any of your bills online?

If you said yes to any of the questions above, you in fact own digital assets.

What are Digital Assets?

What are Digital Assets?

- Almost anyone who uses the internet or a smart phone has digital assets, whether they realize it or not
  - These assets are in the form of digital photos, social networking accounts, emails, cryptocurrency, and more…
- Generally, Digital assets fall into three categories:
  - Digital Assets with Objective Financial Value
  - Non-Financial Digital Assets
  - Electronic Communications

1. Digital Assets with Objective Financial Value

- Cryptocurrency (bitcoin, ether, stablecoin, etc.)
- Loyalty programs (points/miles)
- Virtual property (gaming property)
- Non-fungible tokens
- Electronic blogs/domain names & contents

2. Non-Financial Digital Assets

- Digital photos
- YouTube, TikTok uploads
- Social media accounts
- Electronic medical records
- Electronic tax records
- Electronic banking/finance records
- Cloud storage

3. Electronic Communications

- Emails
- Instant messages
- Texts
- The autopay economy…

The Autopay Economy

- Web-based media (magazines, newspapers, blogs, etc.)
- Software (Adobe Photoshop, CleanMyMac, Malwarebytes)
- Carwash
- Apple TV, YouTube TV, Netflix, Prime, Disney+
- Cloud Storage
- Utilities (water, trash, electricity, gas)
- Health clubs
- Lawn service
- Pest control
- Charities
- Apple music
- Audible (audio books)
- Cell phones

4. Hardware

- Phone
- Tablet
- Personal computer(s) and external hard drive(s)
- Kindle
- Apple Watch/Fitbit

Digital Footprint

- Digital assets with objective financial value +
- Non-financial digital assets +
- Electronic communications +
- Hardware

Why plan for Digital Assets?

Why Plan for Digital Assets?

- Preserve financial value of estate.
- Prevent identity theft.
- Ensure access to and preservation of items with sentimental value (i.e., phots, messages).
- Manage decedent’s social media presence.
- Maintain privacy / ensure your wishes are executed as intended.
- Lessen burden on personal representative and loved ones.

Your role as a fiduciary

Legal Background

- Historically, access to many digital assets were subject to an “End User Agreement”.
  - The automatic “yes” we give when presented with a software terms of service agreement.
- State laws were inconsistent, had conflicting interpretations and generally did not allow concrete authority to access digital information to fiduciaries.

Legal Background

- 2012: The Uniform Law Commission (ULC) created a committee to study the situation.
- 2014: Uniform Fiduciary Access to Digital Access Act (UFADAA)
  - Granted fiduciaries access to digital assets as to other traditional property.
  - Problem: Inconsistent with User's Terms of Service, privacy and possibly Fraud laws.
  - Ultimately not embraced by the states.

Legal Background

- 2015: Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)
  - Grant fiduciaries legal authority to manage digital assets in the same way they manage tangible assets and financial accounts.
  - Grant custodians of digital assets legal authority to deal with the fiduciaries of their users.
  - The general goal of the Act is to facilitate fiduciary access and custodian disclosure while respecting the privacy and intent of the user.

Hierarchy to Fiduciary access to Digital Assets under RUFADAA

- Tier 1 – Online Tools
  - User's affirmative use of on-line tool to grant/deny access controls
  - If online tool allows user to modify or delete a direction at all times, the online tool overrides other contrary directions

- Tier 2 – Written Directions
  - If online tool is not used or one is not provided:
    - Direction can be provided in a Will, Trust, Power of Attorney, or other Record
    - Disclosure to the fiduciary may be allowed or prohibited

Hierarchy to Fiduciary access to Digital Assets under RUFADAA

- Tier 3 – Terms of Service Agreements (TOSA)
  - Use of Tier 1 or Tier 2 overrides contrary terms in a TOSA that does not require the user to act affirmatively and distinctly from the user's assent to the TOSA generally
  - RUFADAA does not change or impair the rights of the custodian or user under a TOSA to access and use the digital assets
  - RUFADAA does not expand the fiduciary's rights beyond those of the user

Action Items & Best Practices

Action Items & Best Practices

- Where appropriate, discuss as part of client reviews.
  - Inform clients about the issues that can arise concerning digital assets and encourage them to prepare.

Important talking point: Your personal representative needs to know about your digital footprint, but it’s equally important that they have the authority to access it when appropriate. Either, without the other is insufficient.

  - When was your estate plan last reviewed?
  - Look for plans created before 2014, as they may need to be updated to align with RUFADAA.

5 best practices to work through with clients

1. Minimize size of Digital Estate:
   - Consolidate where possible.
   - Cancel / close unused sites.
   - Move any files stored on employer’s computer.

2. Understand what you own
   - A digital asset or a license to use the asset?

3. Strategically spend down, or where permissible transfer, airline/hotel rewards
   - Points / Miles are not your property.

5 best practices to work through with clients

4. Inventory
   - Usernames and Passwords (don’t forget devices)
   - Email Accounts
   - Auto bill subscription services
   - Cryptocurrency

5. Check legacy settings on social media

Policies

Social Media

- Facebook
  - Memorialization and Legacy Settings
  - Memorialize or Delete
  - Designate a Legacy Contact
  - Data Archive Permission (download)
  - Delete after death

Social Media

- LinkedIn
  - Profiles of deceased members can be removed or memorialized.
  - The request may be initiated by someone with legal authority to act on behalf of the deceased and who has the proper documentation.
  - Memorialized accounts allow a person’s legacy to remain on LinkedIn after they’ve passed away. A memorialized badge appears on the profile page as a symbol of remembrance.
  - Once an account is memorialized, access to the account is locked.
  - LinkedIn does not disclose usernames or passwords to anyone, including family members, under any circumstances.
  - Non-authorized individuals may simply report a user as deceased.

Apple

iCloud

- Digital Legacy Program
  - Add one or more contacts to access and download certain data in your account after your death.
  - This includes Mail, Contacts, Calendars, files in iCloud drive.
  - It does not include licensed media (movies, music, books) , in-app purchases, or payment and password information.
  - Three-year window beginning when legacy access request is approved. After three years the account is deleted.

Airline Loyalty / Reward Programs

- American Advantage:
  - Your AAdvantage® account will terminate upon your death.

- Southwest Rapid Rewards
  - Points may not be transferred to a Member's estate or as part of a settlement, inheritance, or will. In the event of a Member's death, his/her account will become inactive after 24 months from the last earning date (unless the account is requested to be closed) and points will be unavailable for use.
  - A Member has the ability to transfer points to another Member or a preselected charity chosen by Southwest with an active Rapid Rewards account

Hotel Loyalty / Reward Programs

- Marriott Bonvoy
  - In the event of a Member's death, the Company may, in its sole discretion, allow unredeemed Points from the deceased Member's Account to be transferred to a family member or a friend who is an active Member upon the Company's receipt and review of all requested documentation and communications. Awards, hotel stays, Elite Membership Status, Lifetime Membership Status, and the related benefits, including, without limitation, Elite Night Credit, will not transfer to the recipient of the Points.
- Hilton Honors
  - In case of the death of a Member, Points in the Member's account may be transferred to another active Member upon Hilton Honors receipt and approval of certain requested documentation and information. To be eligible, transfer must be requested, and all required documents and information provided within one year from the date of the Member's death. Any transfer remains within the sole discretion of Hilton Honors. Any decision made by Hilton Honors in response to a request for transfer is final and not subject to further review or dispute. Elite status cannot be transferred, and Points received by a Member through such a transfer will not count toward Elite status.

Resources & Tools

Summary Overview

Fiduciary Access to Digital Assets: A Practical Guide

To assist our fiduciary clients in navigating the evolving digital assets landscape, Federated Hermes examined the principles of existing fiduciary law in the United States with respect to fiduciary access to client digital assets to develop a guide for use by fiduciaries when engaging with clients.

- The Fiduciary Access to Digital Assets: A Practical Guide brochure reviews the following:
  - What are digital assets?
  - Why is it important a fiduciary to have access to digital assets?
  - When can access be given to a fiduciary?

Fiduciary Access to Digital Assets: A Practical Guide

Federated Hermes

Fiduciary access to client digital assets

For over forty years, Federated Hermes has provided products, services and support to fiduciaries acting on behalf of their clients. Throughout this time, we have endeavored to identify trends and issues that impact the investments, processes and procedures utilized by our fiduciary clients in order to help our clients better-understand the legal issues implicated by such novel or evolving practices. Recently, there has been a keen interest on the part of our clients in understanding the fiduciary implications of accessing their clients' "digital assets."

As more people are using the internet in more ways, digital assets are permeating peoples' lives and relationships, including relationships with their fiduciaries and service providers. Almost anyone who uses the internet or has a smart phone has digital assets, whether they realize it or not. Banks, trust companies and financial professionals acting as fiduciaries on behalf of clients, or dealing with the other fiduciaries appointed by their clients, must understand the issues that arise when fiduciaries need access to the client's digital assets. Clients need to understand and appreciate that their fiduciaries will need both information about their digital assets and the authority to use the information. Either without the other is insufficient.

To assist our fiduciary clients in navigating the evolving digital assets landscape, Federated Hermes engaged the services of William Campbell Ries, Esq. and Carolyn A.W. Whitworth. Esq. of Tucker Arensberg, P.C., to examine the principles of existing fiduciary law in the United States with respect to fiduciary access to client digital assets, and to develop a guide for use by fiduciaries when engaging with clients.

The **Fiduciary Access to Digital Assets: A Practical Guide** brochure reviews the following:

What are digital assets?

Generally, digital assets fall into three categories:

- **Electronic communications** such as emails, instant messages, texts
- **Non-financial digital assets** such as family photos and videos, digitally stored tax or health records, social media accounts and cloud storage
- **Digital assets with objective financial value** such as cryptocurrency, digital securities and other tokenized interests, reward programs and frequent flier miles

Why is it important for a fiduciary to have access to digital assets?

A fiduciary's ability to do its job might be greatly assisted by access — or greatly inhibited by lack of access — to digital assets. When banks and trust companies act as fiduciaries, they likely will need access to digital assets to be certain of appropriately fulfilling their duties, for example:

- When a client dies or becomes incapacitated, someone else needs to know what assets the client owned, what liabilities the client had and what obligations the client had. Digital assets such as Bitcoin accounts or an online investment account that are unknown to and/or cannot be accessed by the personal representative of a decedent cannot be administered and distributed to the client's beneficiaries.
- Bills that an incapacitated client's guardian does not receive because they are delivered to the client's email account that the fiduciary cannot access may not be paid, to the detriment of the client and the client's family.
- A client's family might want to retain the photographs that the client has digitally stored in an online account, and someone needs the authority to access and transfer them to avoid the deletion of the account.
- Digital assets are also particularly susceptible to concerns involving identity theft, property theft and loss of privacy. Without someone having the legal authority and information necessary to monitor and control financial digital assets, or even email or social media accounts, those assets and accounts may be stolen or misused.

When can access be given to a fiduciary?

Fiduciary access is determined by the law of whichever state governs the relationship, together with any applicable federal law.

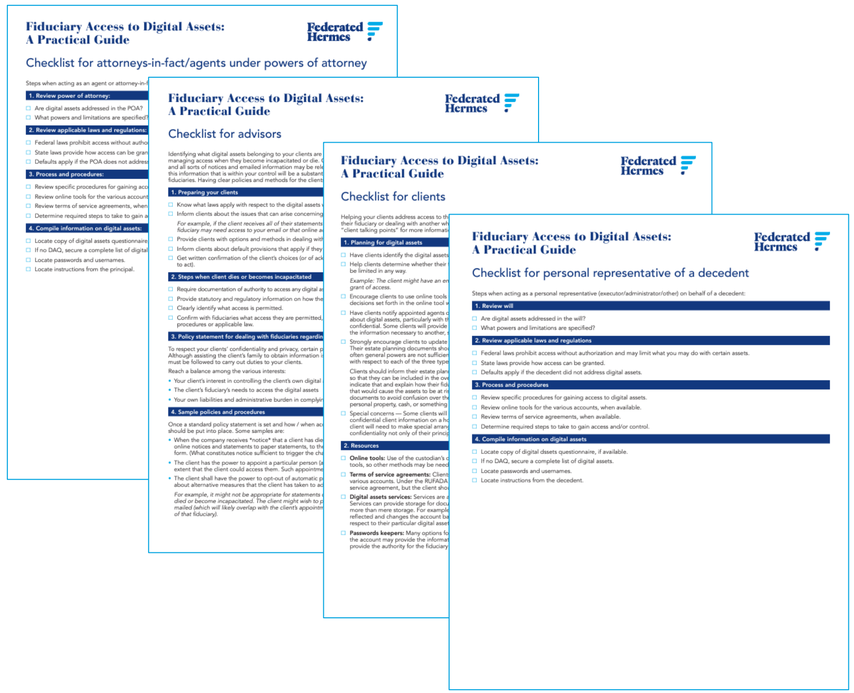
Many state laws provide for a hierarchy of what controls fiduciary access to digital assets. Online tools provided by the custodian, estate planning documents and "Terms of Service Agreements" (TOSA) generally can be used as methods for clients to identify who will have access to their digital assets and to define the scope of access; however these methods may be subject to the limitations imposed by state law. Fiduciaries should be aware of the Revised Uniform Fiduciary Access to Digital Assets Act ("RUFADA Act"), which is currently the basis for such access laws in 45 states, D.C. and the U.S. Virgin Islands, and of applicable federal laws relating to privacy, copyright, data protection and criminal computer fraud.

Continues on next page

Checklists

Identifying what digital assets belonging to your clients are within your control is a first step in determining how to assist your clients in managing access when they become incapacitated or die. Having clear policies and methods for the clients to establish that access is key.

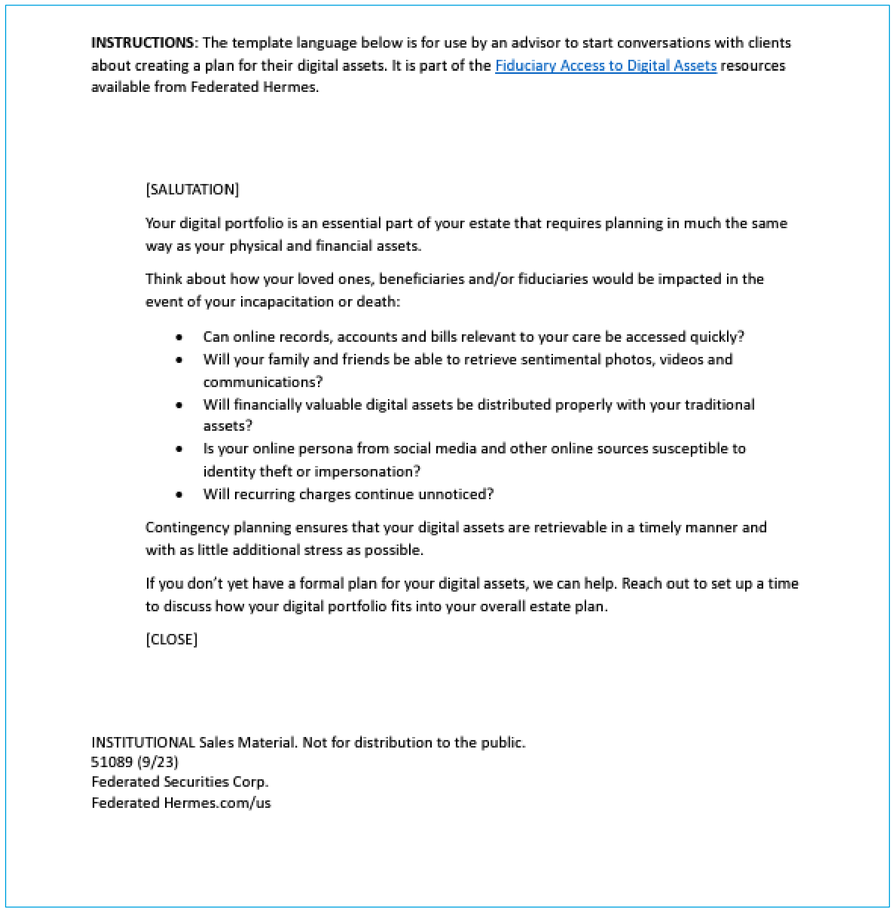
- The following checklists can assist in managing access to your clients' digital assets:
  - Checklist for Advisors
  - Checklist for Attorneys
  - Checklist for Clients
  - Checklist for Executors
  - Checklist for Guardians
  - Checklist for Trustees



Additional Tools and Resources

Client Letter

- In addition to the overview and checklists, we have produced a Client Letter that is ready for use in order to start conversations with clients for their digital assets.



INSTRUCTIONS: The template language below is for use by an advisor to start conversations with clients about creating a plan for their digital assets. It is part of the Fiduciary Access to Digital Assets resources available from Federated Hermes.

[SALUTATION]

Your digital portfolio is an essential part of your estate that requires planning in much the same way as your physical and financial assets.

Think about how your loved ones, beneficiaries and/or fiduciaries would be impacted in the event of your incapacitation or death:

- Can online records, accounts and bills relevant to your care be accessed quickly?
- Will your family and friends be able to retrieve sentimental photos, videos and communications?
- Will financially valuable digital assets be distributed properly with your traditional assets?
- Is your online persona from social media and other online sources susceptible to identity theft or impersonation?
- Will recurring charges continue unnoticed?

Contingency planning ensures that your digital assets are retrievable in a timely manner and with as little additional stress as possible.

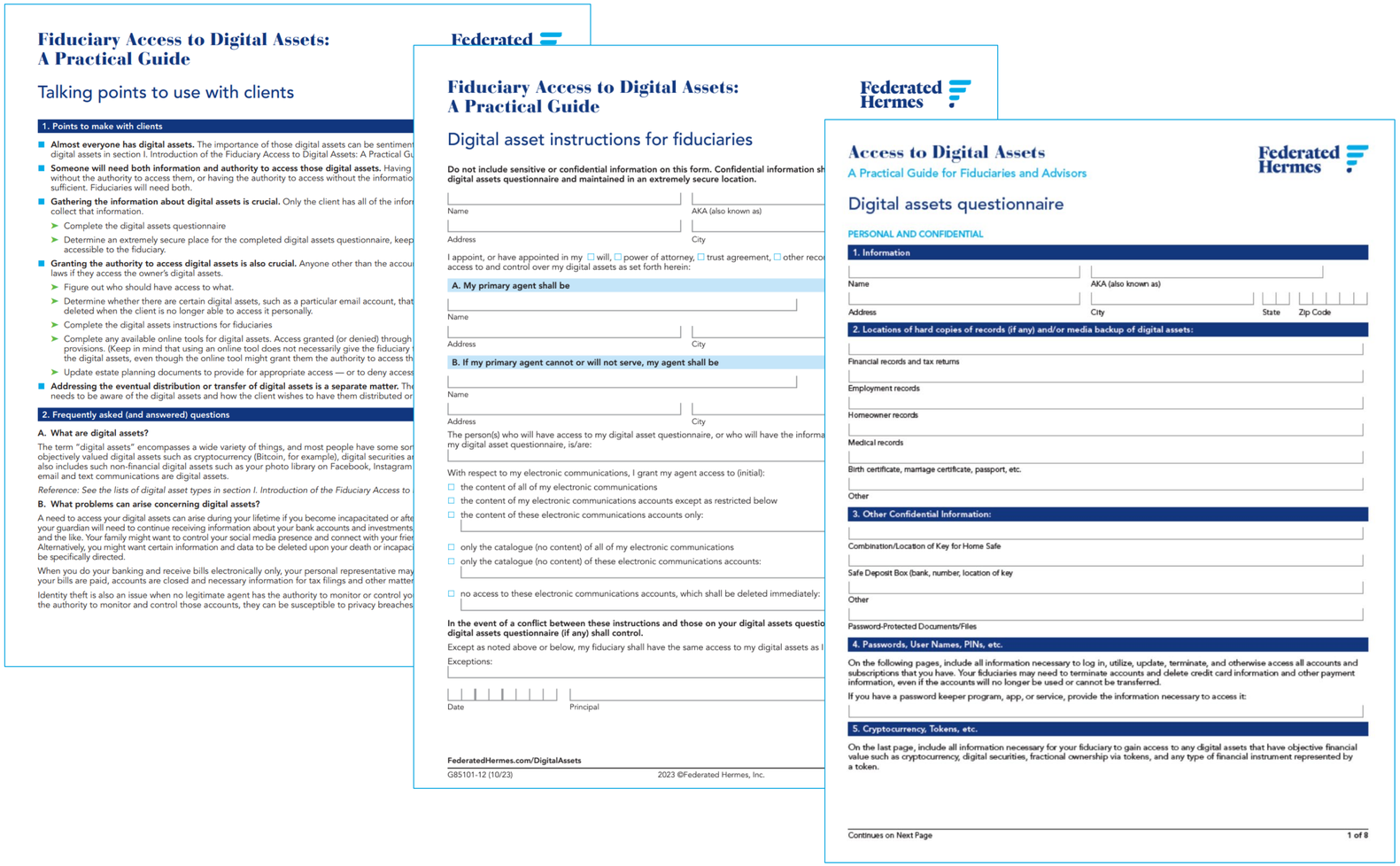
If you don't yet have a formal plan for your digital assets, we can help. Reach out to set up a time to discuss how your digital portfolio fits into your overall estate plan.

[CLOSE]

INSTITUTIONAL Sales Material. Not for distribution to the public.
51089 (9/23)
Federated Securities Corp.
Federated Hermes.com/us

Additional Tools and Resources

- Along with this Client Letter, we also created the following additional tools:
  - Client Talking Point, Digital Assets Instructions, Digital Assets Questionnaire



Fiduciary Access to Digital Assets: A Practical Guide

Talking points to use with clients

1. Points to make with clients

- **Almost everyone has digital assets.** The importance of those digital assets can be sentiment
  digital assets in section I. Introduction of the Fiduciary Access to Digital Assets: A Practical Gu
- **Someone will need both information and authority to access those digital assets.** Having
  without the authority to access them, or having the authority to access without the informatio
  sufficient. Fiduciaries will need both.
- **Gathering the information about digital assets is crucial.** Only the client has all of the infor
  collect that information.
  - Complete the digital assets questionnaire
  - Determine an extremely secure place for the completed digital assets questionnaire, keep
    accessible to the fiduciary.
- **Granting the authority to access digital assets is also crucial.** Anyone other than the accou
  laws if they access the owner's digital assets.
  - Figure out who should have access to what.
  - Determine whether there are certain digital assets, such as a particular email account, that
    deleted when the client is no longer able to access it personally.
  - Complete the digital assets instructions for fiduciaries
  - Complete any available online tools for digital assets. Access granted (or denied) through
    provisions. (Keep in mind that using an online tool does not necessarily give the fiduciary
    the digital assets, even though the online tool might grant them the authority to access th
  - Update estate planning documents to provide for appropriate access — or to deny access
- **Addressing the eventual distribution or transfer of digital assets is a separate matter.** Th
  needs to be aware of the digital assets and how the client wishes to have them distributed or

2. Frequently asked (and answered) questions

A. What are digital assets?

The term "digital assets" encompasses a wide variety of things, and most people have some sor
objectively valued digital assets such as cryptocurrency (Bitcoin, for example), digital securities a
also includes such non-financial digital assets such as your photo library on Facebook, Instagram
email and text communications are digital assets.

Reference: See the lists of digital asset types in section I. Introduction of the Fiduciary Access to

B. What problems can arise concerning digital assets?

A need to access your digital assets can arise during your lifetime if you become incapacitated or afte
your guardian will need to continue receiving information about your bank accounts and investments
and the like. Your family might want to control your social media presence and connect with your frie
Alternatively, you might want certain information and data to be deleted upon your death or incapac
be specifically directed.

When you do your banking and receive bills electronically only, your personal representative may
your bills are paid, accounts are closed and necessary information for tax filings and other matter

Identity theft is also an issue when no legitimate agent has the authority to monitor or control yo
the authority to monitor and control those accounts, they can be susceptible to privacy breaches

Fiduciary Access to Digital Assets: A Practical Guide

Digital asset instructions for fiduciaries

**Do not include sensitive or confidential information on this form. Confidential information sh
digital assets questionnaire and maintained in an extremely secure location.**

Name | AKA (also known as)

Address | City

I appoint, or have appointed in my ☐ will, ☐ power of attorney, ☐ trust agreement, ☐ other reco
access to and control over my digital assets as set forth herein:

A. My primary agent shall be

Name

Address | City

B. If my primary agent cannot or will not serve, my agent shall be

Name

Address | City

The person(s) who will have access to my digital asset questionnaire, or who will have the informa
my digital asset questionnaire, is/are:

With respect to my electronic communications, I grant my agent access to (initial):

☐ the content of all of my electronic communications
☐ the content of my electronic communications accounts except as restricted below
☐ the content of these electronic communications accounts only:

☐ only the catalogue (no content) of all of my electronic communications
☐ only the catalogue (no content) of these electronic communications accounts:

☐ no access to these electronic communications accounts, which shall be deleted immediately:

**In the event of a conflict between these instructions and those on your digital assets questio
digital assets questionnaire (if any) shall control.**

Except as noted above or below, my fiduciary shall have the same access to my digital assets as I

Exceptions:

Date | Principal

FederatedHermes.com/DigitalAssets

G85101-12 (10/23) 2023 ©Federated Hermes, Inc.

Access to Digital Assets

A Practical Guide for Fiduciaries and Advisors

Digital assets questionnaire

PERSONAL AND CONFIDENTIAL

1. Information

Name | AKA (also known as)

Address | City | State | Zip Code

2. Locations of hard copies of records (if any) and/or media backup of digital assets:

Financial records and tax returns

Employment records

Homeowner records

Medical records

Birth certificate, marriage certificate, passport, etc.

Other

3. Other Confidential Information:

Combination/Location of Key for Home Safe

Safe Deposit Box (bank, number, location of key

Other

Password-Protected Documents/Files

4. Passwords, User Names, PINs, etc.

On the following pages, include all information necessary to log in, utilize, update, terminate, and otherwise access all accounts and subscriptions that you have. Your fiduciaries may need to terminate accounts and delete credit card information and other payment information, even if the accounts will no longer be used or cannot be transferred.

If you have a password keeper program, app, or service, provide the information necessary to access it:

5. Cryptocurrency, Tokens, etc.

On the last page, include all information necessary for your fiduciary to gain access to any digital assets that have objective financial value such as cryptocurrency, digital securities, fractional ownership via tokens, and any type of financial instrument represented by a token.

Continues on Next Page 1 of 8

Questions?

Interested in learning more?

Scan the QR Code to check out additional Resources on Digital Asset

Federated Hermes Zone for Digital Assets

Disclosures

This presentation is solely for educational and informational purposes. The information herein is believed to be reliable, but Federated Hermes and its subsidiaries, do not warrant its completeness or accuracy.