BANCROFT

FOR ADVISORS AND THEIR CLIENTS

Digital Asset Inventory Guide

A complete guide to identifying, documenting, and planning for the transfer of digital assets. Covers financial accounts, cryptocurrency, social media, online businesses, subscriptions, credential security, and the legal framework governing fiduciary access.

ABOUT THIS GUIDE

This guide is provided for informational and educational purposes only. It does not constitute legal, tax, or financial advice. Digital asset laws vary by state and are evolving rapidly. Consult with an estate attorney regarding fiduciary access to digital assets in your jurisdiction.

CONTENTS

In this guide

Why Digital Assets Matter

The average person has more than 160 online accounts. Many of these hold financial value, sentimental value, or both. Yet digital assets are routinely overlooked in estate planning. When someone dies or becomes incapacitated, survivors face locked accounts, lost credentials, and assets that may be permanently inaccessible.

160+	$124B	75%
AVERAGE ONLINE ACCOUNTS PER PERSON	ESTIMATED VALUE OF LOST OR INACCESSIBLE CRYPTOCURRENCY	OF ADULTS HAVE NOT PLANNED FOR DIGITAL ASSET TRANSFER

This guide provides a structured framework for identifying every category of digital asset, documenting access information securely, and building a plan that ensures fiduciaries can manage these assets when needed. It is designed as a companion to Bancroft's Asset Inventory Worksheet, which includes a digital assets section for quick documentation.

WHAT QUALIFIES AS A DIGITAL ASSET

A digital asset is any electronic record in which a person has a right or interest. Under the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), this includes:

- Financial accounts accessed or managed online (banking, brokerage, payment apps)
- Cryptocurrency and blockchain assets (Bitcoin, Ethereum, DeFi protocols, NFTs)
- Email accounts (often the key to resetting passwords for everything else)
- Social media profiles (Facebook, Instagram, LinkedIn, X/Twitter, YouTube)
- Cloud storage (Google Drive, Dropbox, iCloud, OneDrive)
- Digital media (music, ebook, photo, and video libraries)
- Online businesses (websites, domain names, e-commerce stores, SaaS products)
- Subscription services (streaming, software, memberships, recurring charges)
- Loyalty and rewards programs (airline miles, hotel points, credit card points)
- Intellectual property stored digitally (manuscripts, designs, software code, patents)

> **Digital assets are not just about money.** A family's photo library in iCloud or Google Photos may be the most emotionally valuable asset in the entire estate. Losing access to decades of family photos, videos, and messages because no one had the password is a loss that cannot be undone. The inventory process should capture sentimental assets alongside financial ones.

Financial Accounts

Online banking, brokerage, and payment accounts are often the most financially significant digital assets. While these accounts are covered by traditional estate planning (beneficiary designations, TOD/POD registrations), the ability to access and manage them online is a separate concern.

ACCOUNTS TO DOCUMENT

CATEGORY	EXAMPLES	WHAT TO RECORD
Online banking	Chase, Wells Fargo, credit union portals, Ally, Marcus	Institution, account numbers, login URL, username, whether 2FA is enabled and method (SMS, authenticator app, hardware key)
Brokerage / investment	Schwab, Fidelity, Vanguard, Robinhood, E*TRADE	Firm, account numbers, login URL, username, beneficiary designations, whether TOD is registered
Payment apps	Venmo, PayPal, Zelle, Cash App, Apple Pay	Username/email, linked bank accounts, current balances, pending transactions
Tax and accounting	TurboTax, H&R Block, QuickBooks, FreshBooks	Login credentials, linked accounts, stored documents (prior returns, 1099s, W-2s)
HSA / FSA portals	HealthEquity, Optum, WageWorks	Account numbers, current balances, designated beneficiaries

Cryptocurrency and Blockchain Assets

Cryptocurrency requires special attention because it operates outside of traditional financial institutions. There is no bank to call. If the private keys or seed phrases are lost, the assets are permanently unrecoverable.

Lost credentials means lost assets, permanently. An estimated $124 billion in Bitcoin alone is considered lost or inaccessible due to missing private keys. Unlike a bank account, there is no institution that can reset your password or verify your identity. If a client holds cryptocurrency, the access documentation is the entire estate plan for those assets.

ASSET TYPE	WHAT TO RECORD	ACCESS NOTES
Exchange accounts (Coinbase, Kraken, Binance, Gemini)	Platform, email, username, 2FA method, account verification status	Major exchanges have bereavement processes. Death certificate + letters testamentary/court order typically required.
Hardware wallets (Ledger, Trezor, Coldcard)	Device location, PIN, seed phrase (12 or 24 words), passphrase if used	Seed phrase is the master key. Without it, the device PIN alone is not enough for recovery.
Software wallets (MetaMask, Trust Wallet, Phantom)	Wallet addresses, seed phrase, password, device where installed	Software wallets exist on a specific device. Document which device and how to access it.
DeFi positions (lending, staking, liquidity pools)	Protocol names, wallet addresses connected, positions held, governance tokens	DeFi has no customer support. The connected wallet is the only access. Document all protocols and the wallet used.
NFTs (art, collectibles, domain names)	Marketplace (OpenSea, etc.), wallet addresses, estimated values	Owned by the wallet, not the marketplace. Same seed phrase recovery as other wallet assets.

Multi-signature and social recovery wallets. Some clients use multi-signature wallets that require 2-of-3 or 3-of-5 key holders to approve transactions. Document all signatories and the threshold. Social recovery wallets (e.g., Argent) designate "guardians" who can help restore access. Confirm that guardians are documented and aware of their role.

Communication and Personal Accounts

Email accounts

Email is often the most critical digital asset to access first, not because of the emails themselves, but because email is the recovery method for virtually every other account. Gaining access to a decedent's primary email unlocks password resets across all linked services.

PROVIDER	LEGACY / BEREAVEMENT PROCESS	WHAT TO DOCUMENT
Google (Gmail)	Inactive Account Manager lets users pre-configure what happens. Without it, Google reviews requests case-by-case with court order.	Email address, recovery phone, recovery email, whether Inactive Account Manager is enabled
Apple (iCloud)	Digital Legacy Program allows pre-designated Legacy Contacts. Without it, court order required.	Apple ID, whether Legacy Contact is set up, device passcodes
Microsoft (Outlook)	Next of Kin process provides limited data from the account with death certificate and proof of relationship.	Email address, linked Microsoft account, recovery methods
Yahoo / AOL	Account closure only. No content access provided to family. Download everything while the user is alive.	Email address, login credentials

> **Activate legacy tools now, not later.** Google's Inactive Account Manager and Apple's Digital Legacy Contact are free, take minutes to set up, and avoid the need for a court order. Every client with a Google or Apple account should configure these during the estate planning process. This is the single highest-impact action in digital estate planning.

Social media

PLATFORM	OPTIONS AFTER DEATH	WHAT TO DOCUMENT
Facebook / Instagram	Memorialize the account (Legacy Contact can manage), or request deletion. Legacy Contact can pin posts and respond to friend requests but cannot read messages.	Account name/URL, whether Legacy Contact is designated, content download preferences

PLATFORM	OPTIONS AFTER DEATH	WHAT TO DOCUMENT
LinkedIn	Memorialization or removal upon request with proof of death.	Profile URL, email associated
X / Twitter	Account deactivation with death certificate. No content transfer.	Username, email associated
YouTube	Handled through Google Inactive Account Manager. Monetized channels may have significant value.	Channel URL, monetization status, linked AdSense account

Cloud Storage and Digital Media

Cloud storage accounts often contain the most emotionally valuable assets: family photos, videos, personal documents, and correspondence. Digital media libraries (music, ebooks, movies) are typically licensed, not owned, meaning they cannot be transferred. But cloud-stored personal content can be preserved with proper access.

SERVICE	TRANSFER / ACCESS NOTES	WHAT TO DOCUMENT
Google Drive / Photos	Covered by Inactive Account Manager. Can auto-share data with designated contacts or delete after inactivity.	Storage used, shared drives, photo library size
iCloud	Digital Legacy Contact can access photos, files, messages, notes, and more. 3-year window after death.	Storage plan, devices linked, Legacy Contact status
Dropbox	No formal legacy program. Account access requires credentials or court order.	Email, plan type, shared folders
Digital media (iTunes, Kindle, Audible, Steam)	Most digital media is licensed, not owned. Apple, Amazon, and most platforms do not allow transfer of purchased content. Download and back up locally where possible.	Platforms, estimated library values, downloaded vs. cloud-only content

Online Businesses and Revenue

Clients who own online businesses, manage websites, or earn revenue from digital platforms hold assets that require active management after death or incapacity. Unlike a bank account that simply sits, an online business may have customers, employees, hosting fees, and domain renewals that need immediate attention.

ASSETS TO DOCUMENT

ASSET TYPE	EXAMPLES	WHAT TO RECORD
Domain names	GoDaddy, Namecheap, Cloudflare, Google Domains	Registrar, domain names, expiration dates, auto-renewal status, registrar login credentials
Website hosting	AWS, Vercel, Netlify, Bluehost, WordPress.com	Provider, login credentials, payment method, server access (SSH keys if applicable)
E-commerce stores	Shopify, Etsy, Amazon Seller, eBay	Platform, store URL, login, linked payment accounts, inventory, supplier contacts
Revenue streams	Google AdSense, Amazon Associates, affiliate programs, Patreon, Substack	Platform, account email, payout method, estimated monthly revenue
Software / SaaS	Self-built apps, code repositories (GitHub), API keys	Repository URLs, deployment credentials, customer database access, revenue metrics

> **Domain names expire.** If a domain name lapses because auto-renewal fails (expired credit card, closed account), the domain enters a grace period and then becomes available to the public. Valuable domains can be registered by squatters within hours. Ensure domain registrar credentials are documented and that someone can access the account to maintain renewals.

Subscriptions and Recurring Charges

Subscriptions cost the estate money every month until somebody stops them, so they have to be documented and cancelled after death. The average American household pays for 12 subscription services. Left uncancelled, these drain estate funds indefinitely.

CATEGORY	COMMON SERVICES	ACTION REQUIRED
Streaming	Netflix, Spotify, YouTube Premium, Hulu, Disney+, HBO Max	Cancel and request final-month refund if applicable
Software	Microsoft 365, Adobe CC, Dropbox, antivirus	Cancel auto-renewal; download stored data before closure
Memberships	Gym, Costco, Amazon Prime, warehouse clubs	Cancel; some offer prorated refunds for remaining term
News / content	NYT, WSJ, Substack, Patreon (as subscriber)	Cancel recurring payments
Insurance (online)	Lemonade, auto-pay policies, supplemental coverage	Notify carrier of death; file claims if applicable before cancelling

Password Management

A password manager is the single most important tool for digital estate planning. It stores all credentials in one encrypted vault, accessible with a single master password. Without a password manager, survivors face the prospect of resetting or recovering hundreds of individual accounts.

RECOMMENDED APPROACH

1. Use a password manager. 1Password, Bitwarden, Dashlane, and LastPass are common options. Store all account credentials here, not in a notebook, spreadsheet, or sticky notes.
2. Document the master password securely. Write the master password on paper and store it with other estate planning documents (e.g., in Bancroft's Digital Safe, a safe deposit box, or with the estate attorney). Do not email it, text it, or store it in another digital account.

3. Enable emergency access. Most password managers offer an emergency access feature that allows a designated person to request access after a waiting period. 1Password has a family plan with shared vaults. Bitwarden offers an emergency access feature with configurable wait times.
4. Back up 2FA recovery codes. For every account that uses two-factor authentication, save the backup/recovery codes in the password manager or with the master password documentation.

The Legal Framework: RUFADAA

The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) has been adopted in all 50 states and the District of Columbia. It provides the legal framework for fiduciary access to digital assets after death or during incapacity.

HOW RUFADAA WORKS

RUFADAA establishes a three-tier priority system for determining who can access a deceased person's digital assets:

1. The user's online tool directions. If the user configured a platform's built-in legacy tool (Google Inactive Account Manager, Apple Digital Legacy, Facebook Legacy Contact), those settings take priority over everything else.
2. The user's estate planning documents. If no online tool direction exists, the will, trust, or power of attorney governs access. The document must specifically authorize digital asset access. General language about "all my property" may not be sufficient.
3. The platform's terms of service. If neither of the above exists, the platform's terms of service control. Most terms of service prohibit access by anyone other than the account holder.

> **Estate documents should explicitly address digital assets.** A power of attorney that says "I grant my agent authority over all my financial accounts" may not be enough to compel Google or Apple to provide access. The document should specifically reference digital assets, electronic communications, and the authority to access, manage, delete, or transfer online accounts. Bancroft's power of attorney templates include this language by default.

WHAT A FIDUCIARY CAN AND CANNOT ACCESS

RUFADAA distinguishes between a "catalogue" of communications (the list of senders, recipients, dates, and subject lines) and the "content" of communications (the actual messages). By default, a fiduciary can access the catalogue but not the content, unless the user specifically authorized content access through an online tool or estate document.

FIDUCIARY TYPE	DEFAULT ACCESS	HOW TO EXPAND ACCESS
Executor / Personal representative	Catalogue of communications; non-content records (purchase history, files, photos)	User configures online tool or will specifically authorizes content access
Trustee	Digital assets held in trust; catalogue of communications related to trust assets	Trust instrument specifically authorizes broader digital asset access
Agent (power of attorney)	Catalogue only; no content access by default	POA specifically grants authority over digital assets and electronic communications
Guardian / Conservator	Catalogue of communications; non-content records necessary for care	Court order authorizing broader access

PLATFORM LEGACY TOOLS: SETUP GUIDE

The following platforms offer free, built-in legacy or inactivity tools. Configuring these takes minutes and eliminates the need for a court order in most cases.

PLATFORM	TOOL NAME	WHAT IT DOES
Google	Inactive Account Manager	After a user-defined period of inactivity (3-18 months), notifies up to 10 designated contacts and can auto-share data (Gmail, Drive, Photos, YouTube) or delete the account entirely.
Apple	Digital Legacy Program	Designate Legacy Contacts who receive an access key. After death (with death certificate), they can access photos, messages, notes, files, and more for 3 years.
Facebook	Legacy Contact	Designated person can write a pinned post, respond to friend requests, update profile/cover photo. Cannot read messages or remove content. Alternative: request account deletion after death.
Password managers	Emergency Access	1Password (family vault sharing), Bitwarden (emergency access with wait period), Dashlane (emergency contacts). Each has different mechanics. Configure during the planning process.

Naming a Digital Executor

A "digital executor" is the person (or one of the people) authorized to manage digital assets after death or incapacity. This can be the same person serving as executor or trustee, or it can be a separate individual with specific technical expertise.

WHO SHOULD SERVE

The ideal digital executor has three qualities:

1. Technical competence. They should be comfortable with online accounts, password managers, two-factor authentication, and, if the client holds cryptocurrency, blockchain wallets. This is not the role for someone who struggles with email.
2. Trustworthiness. They will have access to email, financial accounts, and private communications. They are a fiduciary and must act in the best interest of the estate and beneficiaries.
3. Availability. Some digital tasks are time-sensitive. Domain names expire. Subscription charges continue. Platform inactivity periods run. The digital executor must be able to act promptly.

> **Consider separating the roles.** A traditional executor handles the legal and financial administration of the estate. A digital executor handles the technical work of accessing, managing, and closing online accounts. These skill sets rarely overlap. If the client's executor is not technically sophisticated, name a separate person to handle digital assets and grant them specific authority in the estate documents.

WHAT THE ESTATE DOCUMENTS SHOULD SAY

To ensure the digital executor has proper authority, the will, trust, or power of attorney should include language that:

- Specifically defines "digital assets" to include all electronic records, accounts, and content
- Grants authority to access, manage, continue, or terminate digital accounts
- Authorizes access to the content of electronic communications (not just the catalogue)
- Names the digital executor (if different from the primary executor or trustee)
- Authorizes the digital executor to bypass or override terms-of-service restrictions to the extent permitted by law
- References RUFADAA and the client's state-specific version of the statute

Credential Security Architecture

The fundamental challenge of digital estate planning is the security paradox: credentials must be secure enough to protect the client during life but accessible enough for the fiduciary to use after death. Here is a tiered approach that balances both.

RECOMMENDED CREDENTIAL STORAGE

LAYER	WHAT TO STORE	WHERE TO STORE IT
Layer 1: Master access	Password manager master password, device passcodes, primary email password	Sealed envelope with estate attorney, or in Bancroft's Digital Safe. Paper only. Never stored electronically outside the password manager itself.
Layer 2: Recovery keys	2FA backup codes, cryptocurrency seed phrases, hardware wallet PINs	Separate sealed envelope from Layer 1 (so compromise of one does not expose both). Consider a fireproof safe or safe deposit box.
Layer 3: Inventory reference	List of all accounts, platforms, and asset types (no passwords)	Included in the estate planning file. Can be shared with the executor/trustee without security risk since it contains no credentials.

> **Never store seed phrases digitally.** Cryptocurrency seed phrases should never be stored in email, cloud storage, screenshots, or digital notes. A compromised email account or cloud breach can result in immediate, irreversible loss of all associated cryptocurrency. Seed phrases belong on paper or metal, in physically secure locations, separated from the devices they protect.

Action Steps

Digital estate planning is not a one-time event. Accounts change, new services are added, and credentials are updated. The following checklist should be completed during the initial estate planning process and reviewed annually.

INITIAL SETUP

- [ ] Set up a password manager and migrate all credentials into it. Configure emergency access for a trusted person.

- [ ] Configure platform legacy tools: Google Inactive Account Manager, Apple Digital Legacy Contact, Facebook Legacy Contact.
- [ ] Complete the digital asset inventory using Bancroft's Asset Inventory Worksheet or a dedicated digital asset list. Cover all categories in this guide.
- [ ] Document master credentials on paper. Store the password manager master password and device passcodes in a sealed envelope with the estate attorney or in Bancroft's Digital Safe.
- [ ] Secure cryptocurrency access. Write seed phrases on paper or metal. Store in a fireproof location separate from device PINs. Document exchange accounts and 2FA recovery codes.
- [ ] Update estate planning documents to specifically reference digital assets, grant content access authority, and name a digital executor if appropriate.
- [ ] Inform the executor or trustee that a digital asset inventory exists and where to find it. They do not need credentials now, just the knowledge that the plan is in place.

ANNUAL REVIEW

- [ ] Review and update the digital asset inventory for new or closed accounts.
- [ ] Verify that password manager emergency access contacts are current.
- [ ] Confirm platform legacy tool settings have not been reset by software updates.
- [ ] Update stored master credentials if passwords have changed.
- [ ] Review subscription list and cancel unused services.
- [ ] Verify cryptocurrency holdings and that seed phrase storage is intact and accessible.

Loyalty and Rewards Programs

Airline miles, hotel points, and credit card rewards often have significant value but are frequently overlooked. Transferability varies by program:

- Airlines: Most major airlines (Delta, United, American, Southwest) allow transfer of miles to an heir or estate with a death certificate. Some charge a fee.
- Hotels: Marriott Bonvoy, Hilton Honors, and IHG allow transfer to a family member upon death. Hyatt requires contacting member services.
- Credit card points: Policies vary by issuer. Chase Ultimate Rewards, Amex Membership Rewards, and Citi ThankYou points generally allow transfer to an authorized user or estate. Points are forfeited if the account is closed before transfer.

Glossary

Digital asset

An electronic record in which a person has a right or interest. Includes accounts, files, cryptocurrency, and digital media.

RUFADAA

Revised Uniform Fiduciary Access to Digital Assets Act. The legal framework governing fiduciary access to digital assets, adopted in all 50 states and D.C.

Seed phrase

A series of 12 or 24 words that serves as the master key for a cryptocurrency wallet. Losing the seed phrase means permanently losing access to the wallet's contents.

Two-factor authentication (2FA)

A security method requiring two forms of verification (typically password + code from phone or app) to access an account.

Digital executor

A person authorized to manage digital assets after death or incapacity. May be the same as or different from the traditional executor.

Inactive Account Manager

Google's free tool that allows users to designate what happens to their account data after a period of inactivity.

Legacy Contact

A person designated through a platform's built-in tools (Apple, Facebook) to manage or access certain account features after the user's death.
