a bQuest White Paper

Digital Asset Legacy Planning: Why "Knowing the Password" Is No Longer Enough

Contents

Introduction

For today's clients, wealth lives beyond traditional financial accounts, real estate, and other hard assets. It also lives across devices, platforms, apps, and cloud services, often invisibly. From crypto wallets and online bank accounts to email inboxes, cloud photo libraries, subscription services, and social profiles, every client leaves behind a sprawling digital footprint.

That footprint is far larger than most clients and advisors realize. The average American now maintains roughly **240 online accounts**, each representing a potential access dependency. Collectively, these accounts form a digital estate that few families are prepared to manage.

As industry expert Kate Hufnagel, PMP, better known as Founder of The Digital Wrangler®, puts it, "Most families don't realize that one of the most important assets after a death often isn't money, it's access. Without access, even well-funded and organized estates can grind to a halt."

For RIAs, digital asset legacy planning has become a natural extension of fiduciary care. It sits at the intersection of estate planning, cybersecurity, family dynamics, and operational preparedness; and it's an area where advisors can deliver value without crossing into legal or technical overreach. As clients live longer and the complexity of aging increases, incorporating digital planning into a broader longevity planning strategy allows advisors to lead more holistic, forward-looking conversations that strengthen multi-generational relationships and deepen long-term trust.

Accordingly, this white paper equips RIAs with a clear, actionable guide to identifying digital assets, advising clients on access and continuity, and using digital estate planning as both a risk-management and client growth opportunity.

Mapping the Modern Digital Estate

A client's digital life typically spans multiple categories, each with different risks and recovery paths. Financial and "money-adjacent" assets, such as online banking, brokerage portals, bill pay systems, credit cards, loyalty points, and payment apps, are often accessed through a combination of usernames, passwords, email verification, and text-based authentication. If heirs lose control of the client's email account or phone number, they can find themselves locked out of everything else.

Crypto and blockchain-based assets introduce even higher stakes. Wallets, exchanges, seed phrases, hardware devices, and authenticator apps often have no centralized recovery mechanism. “With crypto, there’s no ‘forgot password’ button,” Hufnagel notes. “If the keys are gone or the instructions aren’t clear, the value may be lost forever and no court order can fix that.”

Beyond financial value, clients also leave behind deeply personal digital assets: photos, videos, messages, notes, journals, and creative work stored across cloud platforms and personal devices. These items may have little market value but immense emotional importance, and families are often shocked to learn how difficult they can be to retrieve.

Finally, for business owners and professionals, digital assets extend into company email, CRMs, payroll systems, bookkeeping platforms, and vendor portals. A single inaccessible login can disrupt payroll, billing, and client communications overnight, potentially impacting the business reputation.

Why Legal Authority is No Longer Enough

Many advisors assume that a will or trust resolves digital access issues. In reality, most tech platforms operate under strict privacy laws and user agreements. Even where states have adopted versions of the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), fiduciaries typically need explicit authorization and instruction, and then must still comply with each platform’s internal process.

“Families are often stunned to learn that having the death certificate doesn’t mean instant access,” Hufnagel explains. “Tech companies are protecting user privacy first, even after death. Planning ahead is the only way to reduce friction.”

This is why RIAs should guide clients toward platform-native legacy tools such as Apple’s Legacy Contact and Google’s Inactive Account Manager. These tools allow users to proactively designate trusted contacts and define what data can be shared, dramatically simplifying the process for heirs.

The advisor’s role is not to collect passwords or store sensitive credentials. Instead, it is to help clients separate instructions from secrets. Instructions, such as what accounts exist, where they are located, who should act, and whom to notify, can be documented and shared appropriately. Secrets, such as actual passwords, recovery codes, and seed phrases, must be stored securely, updated regularly, and accessed only through approved mechanisms.

Encouraging the use of reputable password managers with emergency access features is a practical step. Equally important is documenting two-factor authentication recovery paths and ensuring someone will control the client's phone number and primary email account in the event of incapacity or death. As Hufnagel emphasizes, "Email is the skeleton key. If heirs can't get into the inbox, everything downstream becomes exponentially harder."

The Growing Risk of Access Disruption

Digital access risk, however, is not limited to death or incapacity. A growing number of individuals are experiencing severe access disruptions while fully alive and legally competent, often following the theft of a smartphone. In reported cases, thieves obtained a device passcode, changed account credentials, and enabled platform recovery controls that permanently locked rightful owners out of their primary digital accounts. Victims lost access to contacts, photos, work files, financial records, and cloud-stored data, even when identity could be verified, due to security frameworks that prioritize privacy and encryption over individual account remediation.

The impact can be significant, including prolonged business disruption, loss of critical records, and permanent data inaccessibility. These scenarios underscore a key planning reality: control of a client's phone, primary email account, and account recovery mechanisms often determines control of the entire digital estate.

Biometric security features such as fingerprint and facial recognition further complicate digital access planning. While biometrics enhance security during a client's lifetime, they typically cannot be transferred, reset, or legally overridden after death or incapacity.

In many cases, biometric authentication is required to unlock devices, approve credential changes, or access password managers and recovery settings.

Without documented alternatives, such as known device passcodes, designated trusted users, or clearly defined recovery pathways, biometric protections can unintentionally prevent authorized fiduciaries or family members from accessing critical information, even when legal authority exists.

The Advisor's Expanding Role

For advisors, this reinforces the importance of proactive digital planning while clients are alive, including documented account inventories, defined recovery pathways, designated trusted contacts, and education around platform-specific protections. Digital estate planning is therefore not solely a post-mortem exercise, but an essential component of modern risk management and continuity planning.

What Families Face After a Death

When a client dies, heirs must navigate a patchwork of platform-specific requirements. Technology companies and financial institutions commonly require combinations of death certificates, proof of authority (such as letters testamentary or trust documents), government-issued identification, and formal requests, often through dedicated bereavement processes.

Even when access is granted, timelines can stretch into weeks or months. For families already coping with grief, these delays add stress and confusion. Advisors who can explain this reality ahead of time help clients appreciate why digital estate planning matters, and why preparation is an act of care, not paranoia.

Digital Asset Planning as a Strategic Opportunity

For RIAs, digital asset estate planning is more than a value-added service. It can be a powerful growth lever. It is tangible, relatable, and emotionally resonant, making it ideal for client education. Seminars and webcasts framed around themes like "What Happens to Your Digital Life When You're Gone?" or "Protecting Your Family from Digital Chaos" consistently attract strong attendance. These conversations naturally open doors to deeper planning discussions around trusts, powers of attorney, tax coordination, insurance, business continuity, and family governance.

"When advisors help clients organize their digital lives, trust accelerates," Hufnagel observes. "You're solving a problem they didn't even know how to articulate, and that positions you as indispensable."

Some firms are formalizing this into a repeatable offering: a digital footprint inventory, coordination with the estate attorney, implementation support for legacy tools, and an annual review. The result is stronger client relationships, meaningful differentiation, and a clear demonstration that the firm understands modern risk in a digital world. It can also lead to referrals with these complimentary professionals.

For RIAs, digital asset estate planning is most effective when it is treated not as a one-off conversation, but as an integrated component of the firm's planning process. Many advisors begin by introducing the topic during annual review meetings, positioning it as a natural extension of estate, tax, and risk discussions rather than a separate or technical exercise. These conversations often surface gaps clients were unaware of, creating an opening for deeper engagement.

Some firms formalize the process by offering a digital footprint discovery session, designed to help clients identify the scope of their digital assets and access dependencies without collecting sensitive credentials. Advisors can then coordinate with the client's estate attorney and CPA to ensure digital considerations are appropriately reflected in legal documents, fiduciary designations, and tax planning, reinforcing the advisor's role as the central planning quarterback.

Providing clients with clear educational materials and practical guides further reduces friction and empowers families to take action. Many RIAs are also finding success by hosting client seminars, webcasts, or small-group events focused on digital estate planning, which serve both an educational purpose and a relationship-building function. These events often resonate strongly with clients and prospects alike, as they address issues that are both highly personal and increasingly unavoidable.

As firms refine their approach, digital asset planning can be incorporated into onboarding for new clients and offered as part of an ongoing service tier, complete with an annual "digital refresh" to account for new accounts, devices, and platforms. Over time, advisors can track client engagement with these services as a meaningful indicator of relationship depth and long-term retention, while also identifying opportunities to expand into broader estate, tax, and family governance conversations.

Conclusion: The Future of Fiduciary Care is Digital

Digital asset estate planning has become an essential part of serving modern clients, as more of their wealth, identity, and personal history lives online. Advisors who bring clarity to this complexity help families avoid unnecessary loss and stress, while strengthening relationships through guidance that feels deeply relevant and timely. The opportunity is clear: begin these conversations today, embed digital legacy planning into your standard process, and position your firm as a trusted steward of both the financial and digital legacies your clients leave behind.

Appendix A: Client Digital Asset Inventory Checklist

When to use this: Use this checklist at the start of the planning process to help clients and advisors identify the full scope of a client's digital footprint and understand what exists before making any access or estate-planning decisions. This checklist is designed to surface accounts, platforms, and digital assets that are often overlooked, giving advisors a baseline understanding of where value, access, and risk may reside.

Core Identity & Access
- ☐ Primary email account(s)
- ☐ Backup/recovery email address
- ☐ Mobile phone number (SIM owner and carrier)
- ☐ Devices used regularly (phone, laptop, tablet)
- ☐ Password manager used (if any)
- ☐ Authenticator app(s) in use
- ☐ Location of 2FA recovery codes

Financial & Money-Adjacent Accounts
- ☐ Bank accounts (online access)
- ☐ Brokerage and retirement accounts
- ☐ Credit cards and bill-pay portals
- ☐ Payment apps and digital wallets
- ☐ Loyalty points and rewards programs
- ☐ Online lenders or BNPL accounts
- ☐ Insurance portals

Crypto & Digital Investments (if applicable)
- ☐ Crypto exchanges
- ☐ Self-custody wallets
- ☐ Hardware wallets
- ☐ Seed phrase storage method/location
- ☐ Staking/DeFi/NFT platforms
- ☐ Transaction records location

Cloud, Personal & Legacy Assets
- ☐ Cloud storage (photos, videos, documents)
- ☐ Personal email archives
- ☐ Messaging apps with important history
- ☐ Social media accounts
- ☐ Domain names or websites
- ☐ Creative or intellectual property files

Business & Professional Assets (if applicable)
- ☐ Business email and calendars
- ☐ CRM and client data systems
- ☐ Payroll, bookkeeping, and billing platforms
- ☐ Vendor and SaaS subscriptions
- ☐ Admin access and key staff contacts

Appendix B: Digital Estate Planning Action Checklist

When to use this: Use this checklist once a client's digital assets have been identified to guide concrete next steps, align legal documentation, and ensure responsibilities and access pathways are clearly defined. This checklist bridges discovery and implementation, helping clients move from awareness to action in a structured way.

- ☐ Name executor(s), trustee(s), and agents under POA
- ☐ Confirm fiduciaries are willing and capable
- ☐ Ensure estate documents include digital-asset language
- ☐ Create a digital asset inventory (Appendix A)
- ☐ Separate **instructions** from **passwords/secrets**
- ☐ Choose secure storage for passwords/keys
- ☐ Set up platform-native legacy tools where available
- ☐ Document "what to do first" for family
- ☐ Share location of plan with trusted people
- ☐ Schedule annual digital-asset review

Appendix C: Passwords, Access & Security Checklist

When to use this: Use this checklist when discussing how access will be managed securely, without advisors ever handling credentials directly, and to help clients put proper safeguards in place. This checklist reinforces best practices around passwords, authentication, and recovery while maintaining compliance and minimizing advisor liability.

- ☐ Use a reputable password manager
- ☐ Enable emergency access or legacy access feature
- ☐ Store 2FA backup codes securely
- ☐ Avoid storing passwords in email, notes apps, or spreadsheets
- ☐ Do not reuse passwords across financial accounts
- ☐ Keep phone number and email updated
- ☐ Identify who controls phone/email at incapacity or death
- ☐ Review access after major life events

Appendix D: Executor & Heir First-Steps Checklist

When to use this: Use this checklist to prepare families and designated fiduciaries for what happens immediately after a death, so they know what to do during a highly emotional time. This checklist is intended to reduce confusion, prevent mistakes, and shorten the time it takes for heirs to regain control and stability.

- ◻ Secure the deceased's phone and primary email
- ◻ Obtain multiple certified death certificates
- ◻ Locate will, trust, POA, and digital inventory
- ◻ Contact the financial advisor
- ◻ Freeze or monitor for identity theft
- ◻ Notify key financial institutions
- ◻ Initiate platform legacy/bereavement processes
- ◻ Do not attempt unauthorized logins
- ◻ Track communications and case numbers
- ◻ Ask advisor for coordination support

Appendix E: Platform & Institution Notification Checklist

When to use this: Use this checklist after a death to help executors and heirs systematically notify financial institutions and technology platforms, ensuring nothing critical is missed. This checklist reflects the reality that each institution has its own documentation and process requirements, and that orderly communication matters.

□ Banks and brokerage firms
□ Retirement plan providers
□ Crypto exchanges
□ Credit card issuers
□ Insurance companies
□ Email and cloud providers
□ Social media platforms
□ Subscription and billing services
□ Employers and benefits administrators

Typical documentation requested:
□ Death certificate
□ Proof of authority (executor/trustee documents)
□ Government-issued ID of requester
□ Platform-specific request forms

Appendix F: Annual Digital Estate "Refresh" Checklist

When to use this: Use this checklist as part of an annual client review to ensure digital asset planning stays current as accounts, devices, and technologies change. This checklist helps prevent digital estate plans from becoming outdated and reinforces digital planning as an ongoing process, not a one-time event.

- ☐ Review digital asset inventory
- ☐ Update account list and URLs
- ☐ Confirm legacy contacts and access settings
- ☐ Rotate passwords if needed
- ☐ Update device list
- ☐ Verify phone number and email access
- ☐ Review crypto storage and keys
- ☐ Confirm executor/agent contact details
- ☐ Revisit instructions document
- ☐ Notify advisor of major changes