

The Access Problem: When Clients (or Their Families) Cannot Reach What Matters

A client departs New York for business on a morning flight and is in London by the evening of the same day.

Midair, they receive a potential fraud alert from their bank. Once back on the ground, they biometrically unlock their banking app on a train ride to the hotel and chat with a customer service rep in the States in real time. Later that evening, they meet colleagues for dinner and tap their smartwatch to pay the bill.

Back at the hotel, they try to access work documents on the cloud to prepare for the next day's presentation, but something is wrong.

Unbeknownst to them, the same new-location logins that triggered their bank's fraud alert have also tripped their company's security system, which flags sign-ins from unfamiliar countries or devices as potential threats and locks the account until identity is reverified.

They are locked out of their account. Everything they need is stored digitally. They do not have physical copies of a single document. If they cannot log in, the entire trip could be for nothing.

Panic starts to set in. What now?

While a digital lockout could derail a business trip, an estate planning emergency could have even greater consequences.

The Estate Planning Digital Paradox

An irony of modern estate planning is that the more secure we make our digital lives, the more vulnerable we are to a total planning lockdown when a crisis hits.

Security features such as biometrics, multifactor authentication (MFA), and encryption do their jobs perfectly: They keep bad actors out. But in a medical or travel emergency, these same defenses can completely lock out fiduciaries and family members.

When a crisis strikes, legal authority alone is no longer enough. A power of attorney or trust agreement means nothing if the designated agent cannot bypass a text-message verification screen. A plan is not worth the paper it is written on if the right people cannot reach the right resources behind a digital lockscreen.

Tracking the Digital Access Chain

A client may know every one of their passwords, make this information available to their decision-makers, and still face a digital lockout. The real risk often lies in the hidden links of the verification chain:

- **Single-device and identity dependence.** Many accounts are strictly tied to a specific physical device, phone number, or biometric scan (e.g., Face ID). If that device is lost, damaged, or traveling with an incapacitated client, access stops instantly. Account recovery reliant on a single email address that is itself locked behind that unavailable device can trap the entire planning ecosystem in a loop.
- **MFA lockout.** Multifactor authentication adds valuable cybersecurity, but it creates a second locked door in a crisis. A successor trustee may hold the correct master password, but if

their login attempt triggers a verification code sent via text to a smartphone that is locked away with the client's belongings, out of battery, or simply out of signal range in a foreign country, the fiduciary is effectively locked out.

- **Location-based restrictions.** Financial fraud algorithms are designed to flag anomalous behavior. A login attempt from another country, an unfamiliar device, or an unexpected IP address can trigger automated fraud controls, demanding additional identity challenges or imposing a temporary account freeze.
- **Institutional verification delays.** Even when a decision-maker holds clear legal authority, the institution itself can become a barrier. Fiduciaries may face extensive delays while compliance departments require separate proof of identity, internal document reviews, or proprietary security questions before granting administrative access.

The key question is no longer “Who has authority?” but “What does that person need to locate, verify, unlock, or receive before that authority becomes usable?”

How Travel Can Test Financial and Estate Planning

Travel tests the operational mechanics of an estate plan like nothing else. What works from home may not work from somewhere else, so a plan should be stress-tested for accessibility—from both sides of the digital vault:

- **The traveling client lockout.** A client who normally logs in without issue from a familiar device and location may encounter added identity challenges, geographic fraud controls, or an automated freeze while traveling. A foreign IP address, disabled international service, or lost device can result in an account lockout that cuts off access to important financial information or emergency funds.
- **The family or fiduciary lockout.** If a travel emergency leaves the client incapacitated, family members or fiduciaries back home may have the legal authority to step in but encounter access issues. Automated fraud controls do not readily distinguish between an unauthorized user and a spouse, agent, or trustee responding to a crisis. The master password may be known, yet the required verification code gets sent to the client's unreachable phone. Legal authority exists, but the institution continues treating the decision-maker like a stranger while it completes a review.

The accessibility stress test ultimately comes down to a pair of questions:

- Could the client continue to locate, verify, unlock, and use what matters while away?
- If the client could not act, could the right person at home do the same without relying on the client's phone, email, device, or immediate cooperation?

Build an Access Plan, Not Just an Estate Plan

The solution to the digital paradox is not to weaken cybersecurity or spread passwords among family members. It is to build operational redundancy into a structured access system that identifies important accounts and documents, describes where they are stored, and explains how an authorized person can access them when needed.

That system may include secure digital storage, backup authentication methods, recovery instructions, current account and professional contacts, and guidance about who should receive access—and when.

By moving the planning conversation beyond asset allocation to real-world access, advisors can give mobile clients protection that moves with them.

Clients can then hit the road knowing that, whatever happens, their plan will not become the estate planning equivalent of lost luggage.