

Locked Out: Why Travel Can Expose the Weakest Part of Your Estate Plan

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

This digital paradox is not unique to estate planning. We have all experienced technology that is supposed to make life easier but occasionally causes frustration.

Security features such as biometrics, multifactor authentication (MFA), and encryption may work perfectly to keep bad actors out. But in a crisis, they can leave account holders and decision-makers on the outside.

Travel can magnify the problem by separating you from the devices, documents, people, and places you normally rely on to access important information.

Digital Irony in Action: How a Single Trip Can Expose Multiple Access Problems

Consider the following scenario: You depart from New York for business on a morning flight and are in London by the evening of the same day.

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

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

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

You are locked out of your account. Everything you need is stored digitally. You do not have physical copies of a single document. If you cannot log in, the whole 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—such as an illness, injury, or incapacity that leaves your loved ones scrambling to access your accounts, documents, or emergency funds—could have far greater consequences.

Tracking Your Digital Access Chain

You may know every one of your passwords, make that information available to your 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. If that device is lost, damaged, or unavailable because you have lost capacity, access can stop instantly. Account recovery relying on a single email address that is locked behind an unavailable device can trap the entire system in a loop.

- **MFA lockout.** Multifactor authentication adds valuable cybersecurity, but it creates a second locked door in a crisis. Your *successor* (backup) trustee or agent may know the master password, but a login attempt can trigger a verification code sent by text—and if your phone is locked away with your belongings, out of battery, or simply out of signal range in a foreign country, the person trying to help is effectively locked out.
- **Location-based restrictions.** Financial fraud algorithms are designed to flag unusual behavior. A login attempt from another country, an unfamiliar device, or an unexpected IP address can trigger automated fraud controls, additional identity challenges, or a temporary account freeze.
- **Institutional verification delays.** Even when your decision-maker holds clear legal authority, the institution itself can become a barrier. Your agent, trustee, or other trusted decision-maker may face extensive delays while compliance departments require separate proof of identity, internal document reviews, or proprietary security questions to grant access.
- **Physical and organizational barriers.** Not every access problem is digital. Your key estate planning documents may be locked in a home safe or buried in a filing cabinet, and your family may not know which attorney or advisor has the current copy. A document can be properly prepared but offer limited immediate protection if nobody knows where it is or how to retrieve it.

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

Stress-Test Access from Both Sides of the Digital Vault

Travel can test an estate plan like nothing else. What works from home on a familiar device may not work from an airport, hotel, hospital, or foreign country.

Availability, responsiveness, readiness, and accessibility within an estate plan should all be stress-tested against real-world circumstances to determine whether that plan has earned its wings.

Before leaving on a trip, ask yourself the following questions:

- Can you still access important accounts and documents if your usual phone, laptop, or internet connection is unavailable?
- Do you have a fallback way to receive verification codes, confirm your identity, or contact an institution while traveling?
- Could an unfamiliar device, foreign location, or lack of cellphone service trigger a freeze or lockout when you need access?
- If you become unable to manage your affairs, would the right person know that they have been named to act on your behalf and understand what they are expected to do?
- Could that person quickly locate your key documents, account information, professional contacts, and other information?

- Could they verify their identity and establish their authority without relying on your phone, email, device, physical presence, or immediate cooperation?

A plan passes the stress test only if both sides are prepared for an unanticipated situation during your travels. You must be able to activate your plan from afar, and the right person must be able to use the keys when you cannot.

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 documents and legal authority to real-world access issues, we can give your mobile lifestyle protection that moves with you.

Only then can you hit the road knowing that, whatever happens, your plan will not become the estate planning equivalent of a ground delay, misplaced bag, or phrase lost in translation.