THE WEALTH PRIVACY STACK

Privacy Architecture for High Net Worth

2025-2026 EDITION

by TRUCE

TABLE OF CONTENTS

PART 1 — THE FRAMEWORK

SECTION 1: WHY HIGH NET WORTH PRIVACY IS DIFFERENT

The privacy problems an everyday adult faces and the privacy problems a high net worth individual faces look similar from the outside. Both want to keep their address private, both want to keep their phone secure, both want to limit what shows up when someone searches their name.

The reality is different. Once you have meaningful assets, you become a target in ways most people aren't. The threats stop being theoretical and start being specific.

You're a target for civil litigation. Plaintiff attorneys run public records searches before they file. If your assets are easy to find and easy to map to your name, you're a more attractive defendant than someone whose holdings are structured behind entities. This is not about hiding from legitimate creditors. It is about not painting a target on your back for opportunistic suits.

You're a target for kidnap-for-ransom and physical coercion. Wrench attacks (the term for using physical force to extract crypto keys, passwords, or wire authorizations) have surged globally in the last two years. The single largest predictor of being targeted is being publicly known to have wealth. Address compartmentalization is no longer a paranoid choice. It is a physical safety choice.

You're a target for sophisticated financial attacks. SIM swaps, business email compromise, social engineering of your private banker, deepfake voice calls to your assistant. The attackers know exactly who you are and what's worth taking. They've studied your social media. They know your family members' names. They know your travel schedule. The amateur defenses that work for everyday adults fail against this level of attention.

You're a target for stalkers and obsessives in ways most people aren't. Public profile, even mild, attracts unwanted attention. The threshold for "public profile" is low: one viral post, one news article, one industry mention, one large charitable gift. After that, your old address is in their search history.

The asymmetry that defines this game is simple. The cost of finding you needs to be higher than the value of finding you. For a regular adult, basic privacy hygiene raises the cost just enough that almost no one bothers. For a high net worth individual, the value of finding you is high enough that determined adversaries will spend real money to do it. Your defenses need to be commensurately better.

This is what the wealth privacy stack is. Not paranoia. Not extreme measures. A coherent set of structures, infrastructure, and habits that raise the cost of being targeted to a level where the people most likely to come after you choose easier marks instead.

SECTION 2: THE COMPARTMENTALIZATION PRINCIPLE

There is one organizing concept behind everything else in this guide. Compartmentalization.

Compartmentalization means that no single piece of information about you connects to all the other pieces. Your name doesn't connect directly to your home address. Your home address doesn't connect directly to your business. Your business doesn't connect directly to your investment accounts. Your investment accounts don't connect directly to your real estate. Each connection that exists is intentional and limited.

The opposite of compartmentalization is what most people have. One name. One phone number. One email. One address on everything. One LLC owned in their personal name. One bank that knows their entire financial life. A determined adversary who finds any one of these has found all of them.

Compartmentalization breaks that chain. Different addresses for different purposes. Different phone numbers for different purposes. Different entities owning different asset classes. Different banks for different accounts. None of this requires hiding anything from the IRS, your bank, or a court. Banks know who you are. The IRS knows what you own. Courts can pierce anything with a subpoena. What compartmentalization protects against is the casual searcher, the data broker, the contingency attorney, the disgruntled former employee, the stalker, the journalist, the kidnapper studying your routine.

The principle scales. The richer you are, the more compartments you need, and the more carefully you have to manage the boundaries between them. At low seven figures, four or five compartments is enough. At nine figures, you might have thirty or forty compartments and a family office managing the boundaries.

The point of this guide is to walk through what those compartments look like at each level of the stack: address, phone, banking, entities, real estate, vehicles, investments, crypto, insurance. Each one is its own discipline. Doing one without the others gets you a fraction of the benefit. Doing all of them right gets you the full benefit.

Doing them wrong is worse than doing nothing. A poorly structured anonymous LLC that uses your real name on the wrong document doesn't just fail to protect you. It documents your intent to be private, which becomes evidence if you're ever in litigation. A land trust set up by someone who doesn't understand homestead exemptions can cost you your primary residence tax break. A Montana LLC for your daily-driver vehicle, used wrong, becomes tax evasion.

This is why the rest of this guide is framework, not playbook. The shape of the stack is knowable. The implementation has to be specific to your situation, your state, your assets, and your goals. That part requires licensed professionals.

SECTION 3: THE 2026 LANDSCAPE

A brief tour of what's actually moving in the privacy space right now, because the recommendations in this guide depend on the current state of play.

The federal beneficial ownership picture has shifted in favor of privacy. Recent rulings and rulemaking have substantially relaxed federal reporting requirements on who actually owns domestic entities. Domestic LLCs and their owners face significantly lighter beneficial ownership disclosure obligations than was the case eighteen months ago. This is not a permanent state. Appeals are pending. The rule could be reinstated. Anyone setting up entities now should assume this changes and structure accordingly.

State-level transparency is moving the opposite direction in some states. Certain states have introduced or expanded laws that require disclosure of LLC ownership at the state level. The scope of these laws varies (some apply only to entities formed elsewhere and registered in-state, others reach more broadly), and the specifics are still being shaped by veto decisions, amendments, and legal challenges. If you form or operate an LLC in a state with active transparency legislation, your privacy posture is materially different than if you form it in Wyoming or New Mexico. The state-by-state map matters more than ever, and getting the current state of any specific jurisdiction wrong can defeat the structure.

Real estate transparency rules are in active litigation. A federal rule that would have required disclosure of beneficial owners on certain residential real estate purchases through entities was vacated by a federal court earlier this year. The appeal has been filed but no stay is in place, so the rule is currently unenforceable. The current state is more private than it was a year ago. Plan for it to change with the next appellate decision.

Wrench attacks have changed the threat model. Physical coercion attacks against wealthy individuals (especially crypto holders) have surged. The behavioral implication for HNW privacy is significant. The marginal dollar of privacy investment is now better spent on being unfindable than on legal asset protection structures. If a determined adversary can't locate you, the rest of your defenses don't get tested.

Privacy-focused services have professionalized. The category of "privacy as a service" has matured. Privacy-first mobile carriers, dedicated data broker removal services, secure email with hardware key support, multisig crypto custody platforms with insurance and inheritance planning. The infrastructure to actually execute the stack at HNW levels exists in a way it didn't five years ago.

State laws on consumer data are creating real tools. California's universal data broker deletion platform went live earlier this year. The federal patchwork is still messy but for residents of certain states, there are now government-run tools to force data brokers to remove your information. Use them.

The wealth gap in privacy has widened. Average adults have less privacy than ever. HNW individuals who actually do the work have more privacy than was achievable a decade ago. The tools are better. The legal structures are more refined. The infrastructure is more mature. But the gap between "what's possible" and "what people actually have" is the largest it has ever been. Most HNW individuals are operating with privacy structures that are five to ten years out of date.

That gap is where this guide is aimed. Closing it requires building a stack. Building a stack requires understanding the components, the order of operations, and the failure modes.

If you want this stack designed and built for your specific situation, fully private, done for you, with documentation for everything, book a call at trucepriv.co.

PART 2 — THE INVISIBLE INFRASTRUCTURE

SECTION 4: ADDRESS AND MAIL

The foundation of the entire stack is what address you put on what document. Everything downstream (banking, entities, real estate, investment accounts, insurance) carries an address. If that address is your home, you've leaked. If it's the right address for the wrong purpose, you've leaked. If it's flagged in the wrong database, your bank will reject the account.

This sounds simple. It is not. The address layer is where most HNW privacy stacks fail in implementation, because there are at least four different categories of address and each one has its own rules.

There's the legal residence (where you actually live and vote). There's the public-facing address that appears on business filings (typically a registered agent for an LLC). There's the correspondence address that receives mail from banks, brokerages, and counterparties. There's the delivery address for packages and shipments. A coherent stack uses different addresses for different categories, and none of them is your home address except in the most narrowly limited contexts.

The mechanics of this involve several types of providers, each with its own use case and its own pitfalls. Mailbox services let you have a real street address that receives mail and packages. Registered agent services let you have a public-record address for entity filings. Some addresses are flagged in government databases in ways that banks reject. Some addresses appear on people-search sites and defeat the purpose. Some addresses are tied to verification forms that become discoverable in litigation. Selecting the right address for each purpose, and routing each type of correspondence to the right one, is most of the work.

The pattern that works has multiple addresses operating in parallel, none of them your home, each one routed to a destination you actually control, with mail consolidated and forwarded under a process that doesn't recreate the linkage you spent money to break. Done right, your real address never appears on any document that becomes public, leaks in a breach, or gets sold to data brokers.

Done wrong, you have a CMRA flag on your bank account that triggers a fraud review, or a registered agent address that ends up on a deed, or a forwarding chain that exposes your real address every time you receive a package. The failure modes here are not theoretical. They are the things that catch HNW individuals who tried to do this themselves.

If this is the foundation of the stack and most people get it wrong, the right move is to have a professional design the architecture. The cost of a botched address layer is everything downstream of it.

SECTION 5: PHONE AND COMMUNICATIONS

If address is the foundation, phone is the spine. Almost every modern attack on HNW individuals routes through their phone number at some point. SIM swap to drain accounts. Spoofed calls to compromise their banker. Tracked location data sold by carriers. Text messages used to verify wire transfers.

The phone layer of an HNW stack has several elements that work together. There is the primary cellular service, which should not be in your real name with your real address on file. There are the multiple phone numbers used for different purposes (banking, business, family, public). There is the carrier-level defense against SIM swaps. There is the email infrastructure that backs up your phone (because your email password reset typically goes to your phone, and your phone password reset typically goes to your email).

The general shape of what good looks like at the phone layer involves separating numbers by function. The number your bank has is not the number on your business card. The number on your business card is not the number your family uses. The number your family uses is not the number you give to merchants and apps. Each number is in a different system. A compromise of one doesn't cascade.

The carrier layer matters more than people realize. There are now privacy-first mobile carriers that operate their own mobile core and offer features that traditional carriers can't. Identifier rotation. SIM swap protection at the network level. Encrypted SMS. Built-in secondary numbers. These are real products in 2026, not vapor. Whether they're right for your situation depends on threat model, but for HNW individuals the calculus has changed.

SIM swap defense has standardized across the major carriers. Port-out PINs, number locks, account PINs. Every carrier offers them. Almost no one sets them. Setting them takes one phone call to your carrier. It is the highest-leverage privacy action available to any phone user, full stop.

The deeper move at the HNW level is to remove your phone number from being a recovery factor or 2FA factor on any financial account. Hardware security keys on banking and brokerage. App-based authenticator codes for everything else. Once your phone is no longer the recovery vector for your financial accounts, a SIM swap becomes annoying instead of catastrophic.

The email backing all of this matters. A secure email provider with hardware key 2FA, separate from your personal email, used for your financial relationships, is non-negotiable at HNW levels. The provider matters less than the discipline.

What gets people in trouble is doing one piece without the others. SIM lock without secure email. Hardware keys on banking but the email password is still SMS reset. Privacy-focused carrier but the number is on file with thirty merchants. The phone layer fails as a chain, not as a wall. Any unprotected link defeats the rest.

SECTION 6: BANKING

Banking compartmentalization is a quiet form of privacy that most HNW individuals get half-right. They have a private bank for their primary relationship, but their checking, savings, brokerage, and operating accounts are all at the same institution. One subpoena, one breach, one disgruntled employee, and the complete picture of their financial life is exposed.

The privacy goal at the banking layer is not to hide from your bank. Banks are required by federal customer due diligence rules to verify who you are and beneficially owns any entity opening an account. They will collect your identification, your tax ID, your address, your source of funds. This is non-negotiable and trying to circumvent it crosses into territory you don't want to be in.

The privacy goal is to limit who else has the full picture. Multiple banks. Different banks for different functions. Different addresses on different statements. Different entities owning different accounts. So that any one breach, leak, subpoena, or social engineering attack reveals one piece of the picture rather than all of it.

The general shape of what this looks like at HNW levels involves an operating account for income and expenses, separate savings and investment accounts (often at different institutions), entity accounts for business and real estate, and a private banking relationship for the largest concentrations. None of these need to talk to each other from the outside. The statements go to compartmentalized addresses (see Section 4). The phone number on file is compartmentalized (see Section 5). The login security is uniformly strong (hardware keys, separate emails).

The address question at the banking layer is more nuanced than it sounds. Banks have become more sophisticated about address verification. Certain types of mailbox addresses are flagged in their systems and trigger fraud reviews. Certain types of business addresses look acceptable to a casual reviewer but get flagged by automated systems. Selecting the right address for each bank account requires knowing which categories work for which institutions, which is a moving target.

Private banking adds a layer that's less about technical privacy and more about operational privacy. Fewer hands on your file. A dedicated banker who knows you and isn't reading from a script. Direct lines of communication that don't route through call centers where social engineering happens. This isn't legal anonymity. It's reducing the attack surface of who can access your account information through normal channels.

The mistakes here are the usual ones. Same address on every account. Same phone number on every account. Same email on every account. One institution holding the entire picture. SMS 2FA on financial accounts. Account opening done in person with your driver's license that has your home address on it. Each of these is fixable. The fix has to happen across all the accounts at the same time, because compartmentalization only works if it's complete.

The work of designing the banking layer involves which banks for which functions, which addresses on which accounts, which entities own which accounts, and the operational habits that maintain the compartmentalization over time. That's the implementation. It's where a professional earns their fee.

PART 3 — THE ASSET LAYER

SECTION 7: ANONYMOUS LLCS

An anonymous LLC is a limited liability company formed in a state that does not publish the names of its members or managers on the public record. The state knows who you are. The IRS knows who you are. Your bank knows who you are. But a casual searcher, a contingency-fee attorney, a data broker, or a stalker running your name through public records sees only the entity, not the human behind it.

Anonymous LLCs are the workhorse of HNW privacy structures. Real estate, vehicles, investment accounts, operating businesses, intellectual property — all of these can be held by an anonymous LLC rather than by you personally. Once the asset is held by the entity, your name disappears from the public chain of title.

A handful of states allow this. The differences between them matter. Some are cheaper to form, others have stronger reputational value, others have better case law for the entity protections. Each state has its own fees, its own annual reporting requirements, its own public information rules. Choosing the wrong state for your situation can cost you privacy you thought you were buying.

The shape of an HNW LLC structure is rarely one entity. It is usually multiple entities, often stacked, with different entities holding different asset classes. The reasons for stacking are situational: limiting liability between asset classes, simplifying succession, isolating revenue from holdings, separating real estate from operating businesses, providing flexibility for future planning. A real estate holding entity that owns the LLCs that hold individual properties is a different structure than a single operating LLC. Both can be appropriate. Picking the wrong one for your situation creates either insufficient privacy or unnecessary complexity.

A few things matter that aren't always obvious. The address used on the formation documents matters. The registered agent relationship matters. The operating agreement matters (even though it's typically not public). Whether the LLC has an EIN matters. Whether it has a bank account matters. Whether other documents in your life properly reference the LLC (or accidentally reference you personally where the LLC should be named) matters. Any of these going wrong creates leaks that defeat the structure.

The federal landscape on beneficial ownership reporting has shifted recently in favor of LLC privacy, but this is unstable. State-level transparency laws have moved in the opposite direction in some states. The interaction between federal and state requirements changes the privacy math depending on where you form and where you operate. This is the part that requires current professional advice. The right answer six months ago may not be the right answer today.

The mistake people make most often with anonymous LLCs is treating the formation as the whole job. Filing the articles of organization gets you a piece of paper. The privacy work is everything that happens after: opening accounts in the entity's name, putting assets in the entity's name, keeping personal documents from referencing the entity in linkable ways, maintaining the entity in good standing, and integrating it into your broader stack. A formed-and-forgotten entity provides no real privacy and creates a paper trail that hurts you in litigation.

The other mistake is using anonymous LLCs to do things they're not designed to do. They are a privacy tool. They are not a tax shelter. They are not a way to evade legitimate creditors. They are not a substitute for legal asset protection structures (which is a separate area that requires an attorney specializing in that field). They will not hide you from the IRS, from a court with proper jurisdiction, or from a bank conducting customer due diligence. Anyone who tells you otherwise is lying.

What anonymous LLCs do well, when properly set up and maintained as part of an integrated stack, is keep your name off public records that data brokers, civil plaintiffs, and stalkers rely on. That is a real and meaningful privacy benefit. The execution is where the value of professional help shows up.

SECTION 8: REAL ESTATE OWNERSHIP

The single most public document in your financial life is the deed to your home. It carries your name, the address of the property, the date of purchase, the price paid, and the mortgage holder (if any). Property tax records reinforce all of this annually. Anyone with a name and a state can search county records and find your home in minutes.

Real estate privacy is therefore the highest-impact, highest-difficulty area of the HNW stack. Highest-impact because the home address is the master key that connects your personal life to your physical safety. Highest-difficulty because real estate is heavily regulated, locally varied, and full of secondary documents (insurance, utilities, HOA, mortgages, refinances) that can reintroduce your name if any one of them is mishandled.

The general approach involves separating beneficial ownership from public record ownership. Two primary tools are used. One is the LLC, which provides liability separation and (in privacy-friendly states) keeps your name off the entity record. The other is the land trust, which separates the trustee on the deed from the beneficial owner of the property. These tools are often used in combination, with each one handling part of what neither can do alone.

Each tool has constraints. Land trusts are recognized differently in different states. LLC ownership of a primary residence has tax implications that can cost you homestead exemptions or capital gains exclusions if handled wrong. Mortgages add their own complications, because lenders may have due-on-sale clauses that trigger when title transfers to an entity or trust. Insurance has to be restructured to name the entity correctly or coverage gaps appear. Property taxes have to be paid by the right party from the right account or the privacy trail leaks at the tax record.

These are not hypothetical complications. They are the issues that come up in every real estate privacy project. The right approach depends on the state, the property type, whether there's a mortgage, whether it's a primary residence or investment property, your current and future tax situation, and how the property fits into your broader estate plan.

For investment properties (rentals, second homes, vacation properties), the path is generally cleaner. The privacy structures are well-established and the tax implications are more predictable. Many HNW individuals title their investment real estate in entities and trusts as a matter of course, both for liability and for privacy.

For a primary residence, the calculus is more complex. The tax benefits attached to primary residence ownership in your personal name (homestead exemption in many states, capital gains exclusion at sale, mortgage interest deduction handling) often outweigh the privacy benefit of entity titling at lower wealth levels. The threshold at which it makes sense to absorb those tax costs in exchange for residential privacy depends on your situation. Public profile, threat model, family situation, and overall stack all matter.

The federal regulatory landscape on real estate ownership through entities has been in flux. A rule that would have required disclosure of beneficial owners on certain residential purchases through entities was recently vacated in court. The appeal has been filed but no stay is in place, so the rule is currently unenforceable. The current state is more private than it was. This is unstable and could change with the next appellate decision.

The execution of real estate privacy is the most legally complex piece of the stack. It is the area where the gap between "this is what the structure looks like" and "this is how to actually do it" is largest. It is also the area where mistakes are most expensive and hardest to unwind. If you take only one piece of this guide and decide to hire help on it, this is the one.

If you want this stack designed and built for your specific situation, fully private, done for you, with documentation for everything, book a call at trucepriv.co.

SECTION 9: VEHICLES

Vehicle registration is public record in most states. Anyone with your license plate can run it through a service and find your name and address. Insurance companies tie vehicles to addresses. DMV databases are routinely accessed by law enforcement, private investigators, and (through breaches and improper sales) by parties with less legitimate purposes.

The general approach to vehicle privacy is the same as real estate. Title the vehicle to an entity instead of to you personally. Insure it appropriately. Register it in a jurisdiction that allows entity ownership without exposing the beneficial owner.

This is where a specific and important caution is required. There is a well-known structure involving titling vehicles to an LLC in a state with no sales tax and no inspection requirements, while the vehicle is actually used in the owner's home state. Several states have begun aggressively prosecuting this structure as tax evasion. Investigations are running into the hundreds, criminal charges have been filed, and recovery actions are recovering millions in unpaid taxes and penalties. The states using this approach include some of the largest by population, and the enforcement involves plate readers, toll tag data, and interagency data sharing.

The privacy structure of "title your daily driver to an out-of-state LLC to avoid sales tax" is, in 2026, a tax evasion exposure first and a privacy strategy second. It is not appropriate for any reader of this guide who would actually be driving the vehicle primarily in their home state. The legal exposure outweighs the privacy benefit and creates the kind of paper trail that defeats privacy goals if you end up in court.

The legitimate approaches to vehicle privacy involve titling vehicles to an entity that is appropriate for your actual jurisdiction, paying the taxes that are actually owed in the state where the vehicle is primarily used, and using the entity structure for privacy rather than tax arbitrage. This is achievable. It requires the right

entity setup and the right insurance.

For collector vehicles, exotic vehicles, or vehicles that are genuinely used primarily in another state, the calculus is different. There are legitimate structures for these situations. The structures look like what the aggressive marketing pushes but are executed legally, in the right context, with taxes properly paid.

For daily drivers, the most common HNW pattern is to accept registration in your own name, focus your privacy investment on other layers of the stack (especially the data broker removal and address compartmentalization), and rely on the broader stack to keep the registration data from being easily linked to other information about you. Privacy through breadth, not just through entity titling.

The insurance side of this matters and is often overlooked. If a vehicle is titled to an entity, the insurance has to properly name that entity and the appropriate drivers. Mismatches between titled owner and policy named insured can void coverage entirely. The cheap way of handling this (a personal auto policy on an entity-titled vehicle) is the most common mistake and the most expensive one when something happens.

The general principle: vehicle privacy is doable, but it has to be done correctly for your specific situation, your specific state, and your specific use case. The off-the-shelf advice circulating online is increasingly a legal exposure rather than a privacy solution.

SECTION 10: INVESTMENT ACCOUNTS

Investment accounts are an underused privacy layer. Most major brokerages allow accounts to be opened in the name of an LLC, trust, or other entity. The statements carry the entity name. The address on file is the entity's address. The beneficial owner (you) is documented internally at the brokerage and on tax filings, but the public-facing footprint is the entity.

The major brokerages all support this with varying requirements. Some have minimum relationship sizes for entity accounts. Some require additional documentation on the entity structure. All of them require the same kind of beneficial ownership disclosure that any other entity account would require. Banks know who you are. The IRS knows what you own. The public-facing privacy is the value.

The general HNW pattern is to hold concentrated investment positions in entity accounts, with the entities matching the broader structure of your stack. Real estate investment entities hold real estate investments. Operating company holdings sit at the operating company. Personal investment accounts sit at personal entities. The compartmentalization principle applies here as it does everywhere else in the stack.

The benefit shows up in several places. Statements with the entity name and entity address don't leak your home address through paper mail or through any future data breach. Beneficiary designations can be structured through the entity rather than directly to family members in ways that show up in probate filings. Brokerage relationships with high asset minimums (private wealth, family office channels) have their own operational privacy benefits in terms of who handles your account and how.

A note that gets overlooked: brokerages, like banks, are subject to customer due diligence and beneficial ownership requirements. They know who actually owns the entity. They have to. The privacy is from the public record and from future data exposure, not from the brokerage itself. Anyone who tells you that an entity brokerage account hides you from the brokerage is misinformed.

The setup is straightforward in concept and detailed in execution. The entity needs to exist, be in good standing, have an EIN, have appropriate operating documents, and have the right address infrastructure. The brokerage will require all of these documents at account opening. The entity has to be the right type of entity for the assets being held, which often means the entity has been chosen with the brokerage account in mind rather than retrofit later. This is the kind of integration work that benefits from being designed end-to-end rather than assembled piece by piece.

SECTION 11: CRYPTOCURRENCY CUSTODY

Cryptocurrency creates privacy problems that don't exist for other asset classes. The blockchain is permanently public. Every wallet address ever used for a transaction is permanently linked to every other wallet address it has transacted with. If any one of those wallet addresses is ever linked to your real identity (through an exchange, a KYC event, a leaked database, or a social media post), the entire transaction history of every connected wallet becomes traceable to you.

This means crypto privacy is fundamentally different from traditional asset privacy. The privacy decisions have to be made before transactions happen, not after. Once a wallet is linked to your identity, it can't be unlinked. You can stop using it, but the history remains.

At HNW levels, crypto custody has reorganized around two related concerns. One is the technical problem of keeping the keys safe. The other is the physical problem of not becoming a target for coercion attacks. The latter has driven the most significant changes in the last two years.

The technical custody question has several layers. Hardware wallets keep keys offline and have been the floor of decent custody for years. Multisig setups (where multiple keys are required to authorize a transaction, with the keys held in different physical locations or by different parties) provide much stronger protection against both technical compromise and physical coercion. Qualified institutional custodians (regulated trust companies and banks that offer crypto custody) handle the institutional end, with insurance and inheritance planning built in.

The choice between these options depends on amount, technical comfort, threat model, and inheritance planning needs. A holder of a meaningful but not life-changing amount in crypto may be best served by a hardware wallet and disciplined operational privacy. A holder of a significant portion of net worth in crypto needs a multisig structure with geographically dispersed keys and a clear inheritance plan. A holder with institutional-scale holdings needs a qualified custodian with the regulatory protections and insurance that come with one.

The privacy side of crypto custody is the part most people get wrong. The technical custody can be excellent and the privacy can still be terrible if your identity is publicly linked to wallet addresses. Common ways this happens: exchange KYC followed by transfers to "private" wallets that are forever linked to your identity, social media posts about holdings or transactions, mentions in interviews or podcasts, leaks from breached exchanges that publish customer wallet addresses alongside KYC data. Any of these creates the link that defeats the rest of your privacy.

The wrench attack problem deserves direct mention. Physical coercion attacks against crypto holders have surged. Kidnappings, home invasions, and assaults specifically targeting individuals known to hold crypto. The single largest predictor of being targeted is being publicly known to hold meaningful amounts.

The privacy implication is that for HNW crypto holders, anonymity is not a preference. It is a physical safety measure. Anyone publicly discussing their holdings, anyone whose holdings have been linked to their identity through a breach, anyone whose wallet addresses are searchable on social media — these individuals are operating with a meaningful physical risk that doesn't exist for crypto holders who have maintained privacy from the start.

The execution of HNW crypto custody is detailed and situation-specific. The right multisig structure depends on family situation, inheritance plans, technical comfort, and amount. The right hardware setup depends on threat model and operational habits. The right institutional relationship depends on amount and use case. Getting any of these wrong is expensive in ways that other privacy mistakes aren't, because crypto losses are typically permanent and the physical safety implications are real.

This is not an area to figure out by reading blog posts. The good news is the infrastructure to do this well exists and is mature. The bad news is the failure modes are unforgiving.

PART 4 — OPERATIONAL

SECTION 12: INSURANCE AS PRIVACY

Insurance is the most underrated component of the HNW privacy stack. It is also the most overrated component of the HNW asset protection conversation. Both things are true at the same time and the distinction matters.

Insurance is a privacy tool because it covers the consequences of privacy failures. When someone runs your information, finds you, and sues you over something opportunistic, your umbrella policy is what pays the defense costs and the settlement. Without it, every privacy failure is also a financial failure. With it, most privacy failures are absorbed before they reach your balance sheet.

The umbrella policy is the foundation. Layers of coverage above your standard auto and homeowners liability limits. The first million of coverage is inexpensive. The second million is also inexpensive. Coverage above five million becomes more involved and may require specialty insurers. HNW families typically carry coverage in the millions to tens of millions depending on net worth and exposure. The cost relative to net worth is small enough that the absence of adequate umbrella coverage is almost always a mistake.

What umbrella policies cover is broader than most people realize. Standard liability for accidents, of course. But also defamation, libel, slander, false arrest, invasion of privacy, and wrongful eviction. These last categories matter directly for HNW individuals because they are the kinds of claims that come up when someone is in the public eye or operating businesses that have public exposure.

The privacy interaction with entity-held assets is critical and frequently mishandled. If a property is owned by an LLC, the LLC has to be a named insured on the policy. If a vehicle is owned by an entity, the entity has to be properly named on the policy. Mismatches between titled owner and policy named insured create coverage gaps that don't get discovered until a claim happens. A botched entity-insurance integration is one of the most expensive mistakes in the HNW stack because it can void coverage entirely after a triggering event.

The other privacy interaction is around the application process itself. Insurance applications collect detailed personal information. High-value home policies, fine art policies, and similar specialty coverages may require inventories and appraisals. This information becomes part of industry databases. Insurance brokerages and carriers have been breached before and will be again. Structuring the insurance relationships with the same attention to compartmentalization that goes into the rest of the stack matters.

What insurance does not do is provide asset protection in any robust sense. It pays claims up to its limits. It does not shield assets from determined creditors, from judgments in excess of coverage, from claims excluded from the policy, or from the universe of risks that aren't covered by liability insurance. Anyone selling insurance as a comprehensive asset protection strategy is overselling. Anyone dismissing insurance as a privacy tool is underselling.

The right approach is to use insurance as the first and most important layer of financial defense, structure it to integrate with the entity layer of the stack, and treat it as the catch-all that absorbs the inevitable failures in the rest of the privacy architecture. Done right, it is the single highest dollar-for-dollar privacy investment most HNW families make.

The execution involves coordinating with insurance specialists who understand HNW exposures, structuring named insureds correctly across all the entities in the stack, sizing coverage to actual risk rather than to net worth (which is a common error), and reviewing coverage as the stack evolves. It is detailed, ongoing work that doesn't lend itself to off-the-shelf advice.

SECTION 13: DAILY OPERATIONAL HABITS

The structures are the architecture. The daily habits are what determine whether the architecture actually holds up over time. Most HNW privacy stacks fail not because the structures were wrong but because the operational habits leak the privacy that the structures provide.

The habits that matter are not exotic. They are the small decisions that get made dozens of times a day. What name goes on this reservation. What address goes on this account. What phone number goes on this form. What card is used for this purchase. What email is used for this signup. What is photographed and posted. What is mentioned in conversations with people who don't need to know it.

The shopping habit. Online purchases that route to the home address, paid with the personal card under the personal name, defeat the structures upstream. The HNW pattern is to use merchant-specific virtual cards (services that generate single-use or merchant-locked card numbers), shipping to a delivery address that isn't the home, with names that don't link directly to other identifiers in the stack. This sounds tedious. With the right tools and a few minutes of setup, it becomes automatic.

The reservation habit. Hotel reservations, dinner reservations, rental cars, all of these create records. The records get sold or breached. HNW individuals with serious privacy posture use business cards on reservations where appropriate, alias names where legal, and avoid the loyalty program registrations that aggregate the most detailed history.

The travel habit. Itineraries that get shared, photos that get posted in real time, social media check-ins, all of these defeat the address compartmentalization upstream. The pattern is to post on delay rather than in real time, avoid geotagged photos near the residence, and keep family informed off-channel rather than through public posts.

The conversation habit. Mentions of net worth, mentions of specific holdings, mentions of upcoming purchases or trips, mentions of address details. These are the things that get picked up by people who are paying attention. The discipline of not announcing wealth is one of the most consistent practices among privacy-aware HNW individuals, and one of the most consistently violated by people who should know better.

The public records monitoring habit. Sophisticated HNW individuals monitor their own public records. Court filings, UCC liens, deed records, business filings under their name. New filings appearing under your name in a state where you don't operate is a warning sign. Setting up monitoring catches identity issues, fraud attempts, and improper use of your name early enough to respond.

The data broker habit. Data brokers re-aggregate your information continuously. Opt-outs aren't permanent. Quarterly or monthly maintenance is the minimum to keep your information off people-search sites. This is now often outsourced to dedicated services, but the work has to happen regardless of who does it. Without ongoing maintenance, the broker data refills over time and undoes the work.

The family habit. The most carefully constructed privacy stack fails if your family members are publicly broadcasting your information. Spouses with public social media that reveals shared location. Children with school records under your name. Parents with obituary mentions naming family. Adult children with vehicles titled in joint names. These are the linkage points that defeat the structure. The conversation with family about what privacy posture to maintain together is uncomfortable and necessary.

Habits compound. Each individual habit feels minor. Together they determine whether the stack is real or theatrical. The HNW individuals who have meaningful privacy a decade after building the stack are the ones who built the operational habits into their daily life. The ones who have nominal privacy have the structures without the discipline.

SECTION 14: COMMON MISTAKES

The most expensive privacy mistakes at the HNW level fall into a small number of categories. Knowing the failure modes is most of what protects against them.

Setting up structures and not retitling assets into them. An LLC with no assets in it provides no privacy. A trust with nothing funded into it serves no purpose. This is the most common HNW privacy failure: paying for the structures and never doing the work of moving assets into them. The structures sit dormant. The owner believes they have privacy. The assets remain titled exactly as they were before. When a search happens, the search finds them.

Believing a revocable living trust provides asset protection. Revocable living trusts are estate planning tools. They are useful for avoiding probate and for some privacy purposes in some states. They are not asset protection. The settlor (you) is treated as the owner of the assets for creditor purposes. Anyone selling a revocable living trust as asset protection is misrepresenting the product.

Joint ownership of assets between spouses or with adult children. Joint ownership doubles the exposure surface. Anything that exposes the joint owner exposes the asset. Adult children with bad driving records, business problems, or litigation create exposure for the joint asset. This is one of the most common HNW exposures because it feels like a natural family structure.

Using personal information on entity documents. An LLC formed in a privacy state with your home address on the operating agreement, your personal email on the registered agent forms, or your personal phone number on the bank account opening defeats the privacy of the entity. Each document is its own link in the chain. The chain is only as strong as the weakest document.

Social media leakage that defeats the structure. The structures keep your name off public records. Social media puts your name on a different kind of public record. Identifying photos, geotagged locations, mentions of holdings, mentions of routine. Each post is a piece of information that an adversary can use to bridge from your social media presence to the structures that hide your assets.

Inadequate insurance coordination with the entity structure. Vehicles titled to LLCs with personal auto policies. Properties owned by entities without the entities named on the policies. Umbrella policies that don't cover the structured assets because the named insureds are wrong. These are common, expensive, and don't show up until a claim happens.

Phone-based account recovery on financial accounts. SIM swap defenses have improved. Phone numbers as the recovery vector for financial accounts is still common. Hardware security keys exist. Authenticator apps exist. The transition from SMS recovery to hardware keys is non-negotiable at HNW levels and is still skipped by most HNW account holders.

One bank, one email, one phone, one address for everything. The compartmentalization principle violated. One subpoena, one breach, one social engineering attack, and the entire picture is exposed. This is the default state for most HNW individuals before they intentionally restructure.

Treating data broker removal as a one-time project. Removing your information from data brokers once, declaring victory, and not maintaining it. The data refills over time. Maintenance is permanent. Without ongoing work, the structures upstream become irrelevant because your name and address are back on the broker sites.

DIY where DIY is dangerous. Some parts of this stack are achievable yourself. Other parts are technical legal work where the cost of errors is very high. The pattern of trying to save fees on the legal parts and discovering the mistakes years later, after they've calcified into other documents and structures, is common and very expensive to unwind.

Trying to use privacy structures to do things they're not designed to do. Anonymous LLCs to evade taxes. Trusts to hide assets from legitimate creditors. Out-of-state vehicle titling to avoid taxes legitimately owed. Each of these creates legal exposure that dwarfs the privacy benefit and creates the kind of paper trail that hurts in litigation. Privacy structures are privacy tools. They are not tax planning, not creditor protection, and not tools for avoiding legitimate obligations. The HNW individuals who get this wrong end up worse off than if they had done nothing.

The pattern across all of these is that privacy isn't a set of products you buy. It is an integrated architecture that has to be designed, implemented, and maintained. Off-the-shelf advice and individual products are necessary but not sufficient. The work is in the integration.

If you want this stack designed and built for your specific situation, fully private, done for you, with documentation for everything, book a call at trucepriv.co.

PART 5 — THE STACK BY NET WORTH

SECTION 15: LOW SEVEN FIGURES

At one to five million in net worth, the privacy stack is achievable, mostly DIY-able for the operational pieces, and best implemented over the course of months rather than weeks.

The architecture at this level focuses on the highest-leverage, lowest-complexity pieces first. Adequate umbrella coverage. Removal from data brokers. Address compartmentalization through a mailbox service. Phone compartmentalization with multiple numbers. Hardware security keys on financial accounts. Secure email separate from personal email. Credit freezes at all three bureaus. SIM swap defense at the carrier level.

For most individuals at this level, the home is held in personal name or in a revocable living trust for probate avoidance. Entity structures for the primary residence are usually not cost-justified at this level because the homestead and capital gains tax benefits typically outweigh the privacy benefit. The cost-benefit shifts as you go up the wealth ladder.

Investment properties (rentals, second homes) at this level may justify entity titling. The structures are cheaper to maintain than they are commonly perceived to be. The privacy and liability benefits are real for properties that produce income or have tenants.

The operational habits at this level are most of the work. Discipline about what address goes on what document. Discipline about what phone number goes on what account. Discipline about what gets posted on social media. The habits compound over years. The structures support the habits but don't replace them.

The professional involvement at this level is intermittent rather than continuous. An attorney for entity formation if needed. A CPA who understands the family situation. A privacy professional to design the architecture and set the operational habits. After the initial setup, the maintenance is mostly self-managed with a quarterly review.

The mistake people at this level make most often is overspending on complexity. Stacked LLCs, multiple trusts, and elaborate structures that cost more in annual fees and complexity than they save in privacy. The right stack at this level is simpler than most people think and more disciplined than most people execute.

SECTION 16: MID EIGHT FIGURES

At ten to fifty million in net worth, the calculus shifts. The privacy stack is no longer something to do yourself. The structures need to be more sophisticated. The maintenance becomes ongoing rather than periodic. The integration across asset classes matters more.

The architecture at this level adds entity ownership of investment real estate as a default, often with land trusts or layered structures depending on state and situation. Entity ownership of investment accounts

becomes standard. Operating businesses are held in dedicated entities separate from personal holdings. Insurance coverage moves to specialty HNW insurers with higher limits and broader coverage. The phone, address, and email infrastructure is built out across more compartments.

The primary residence question becomes more nuanced at this level. The privacy benefit of entity titling becomes more meaningful as the public profile of the owner grows. The tax costs of entity titling can be partially mitigated through specific structures (land trusts with the owner as beneficiary, for example). The decision becomes situational based on threat model and goals rather than a clear default.

The compartmentalization across asset classes becomes more elaborate. Different banks for different functions. Different entities for different asset categories. Different addresses on different accounts. The architecture starts to look like a small institutional structure rather than a personal one.

The professional involvement at this level is continuous. An attorney who specializes in HNW work. A CPA who understands the integrated picture. A privacy professional managing the architecture. Possibly a wealth advisor coordinating across the structures. These professionals work together on the file rather than independently.

The mistake people at this level make most often is not retitling assets after building the structures. The structures exist on paper. The assets remain titled as they were. The privacy benefit is theoretical. This is the most common failure mode at this wealth level: paying for sophisticated structures and not doing the work of populating them. Without the retitling, the rest of the stack is theater.

SECTION 17: NINE FIGURES AND ABOVE

At a hundred million in net worth and above, the privacy stack is no longer a personal project. It is operated by a family office or a dedicated professional team. The structures are bespoke. The maintenance is full-time work for someone other than the principal.

The architecture at this level involves multiple stacked entities, often with elaborate ownership structures that serve privacy, liability, tax, and estate planning goals simultaneously. Asset custody is through institutional channels. Investment management is professional. Real estate is held in structures designed for the specific holdings. Crypto holdings (if any) are held through qualified custodians with insurance. Insurance is layered with specialty carriers up to limits that aren't available to lower wealth levels.

The address and phone infrastructure is similarly elaborate. Multiple physical offices that handle different functions. Personal staff who insulate the principal from most direct contact with merchants, service providers, and counterparties. Travel arrangements made through entities. Public appearances managed through professionals who handle the operational privacy.

The professional team is permanent and integrated. Attorneys, CPAs, family office staff, security professionals, privacy professionals. These individuals know each other and coordinate on the file as a regular practice. The principal makes high-level decisions. The implementation is delegated.

The mistakes at this level are different than at lower levels. Less often about doing the wrong things and more often about staff failures or vendor failures. A breach at a service provider. A new staff member who doesn't understand the privacy posture. A change in family situation that requires restructuring. The maintenance is institutional rather than personal.

The reason this level is mentioned in this guide is to make clear that the stack scales. The principles are the same at every wealth level. The execution becomes more elaborate as the wealth grows. Anyone moving from one level to the next should expect to restructure rather than to add to existing structures. The structures that were appropriate at ten million may not be appropriate at fifty million. The structures that were appropriate at fifty million may need to be replaced at three hundred million.

SECTION 18: WHEN TO HIRE HELP

Most of this guide has been about what the stack looks like, not about how to build it. That is intentional. The how is where professionals earn their fees. The reading of this guide is meant to give you the framework to know whether you have a real stack or a theatrical one, whether your structures are integrated or just collected, whether your privacy posture matches your wealth level or lags it.

The signals that you need help are usually clear once you go looking for them. Your home address appears on people-search sites. Your name appears on title documents that anyone can pull from the county. Your investment accounts come to your home address. Your phone number is on dozens of financial accounts. You have no umbrella policy or one sized to a much lower wealth level than you currently have. You have entities that were formed years ago and never updated. You have assets titled jointly with family members who have their own exposure.

Each of these is fixable. None of them is fixable in isolation. The work has to be done as an integrated project because the pieces interact. Fixing one piece without the others can create more exposure than it removes.

The professional you need depends on your situation. Some pieces of the stack are legal work and require an attorney licensed in your state, particularly anything involving entity formation, real estate titling, trust structures, and tax planning. Other pieces are not legal work but require expertise to do well, particularly the integration of the various components, the operational habits, the technology infrastructure, and the ongoing maintenance.

What I do at TRUCE is the non-legal integration work. The architecture of how the pieces fit together. The phone and email and address infrastructure. The technology setup. The operational habits. The ongoing review. I work alongside your legal and tax professionals rather than replacing them. The legal and tax work is theirs. The integration and execution is mine.

If you don't yet have legal and tax professionals appropriate for your wealth level, getting those relationships set up is the first step. The professional integration is the second step. Building the stack without the right legal and tax foundations creates problems that are harder to unwind than to prevent.

If you have the legal and tax foundations and what's missing is the integrated execution, that's the work I do.

If you want this stack designed and built for your specific situation, fully private, done for you, with documentation for everything, book a call at trucepriv.co.

CLOSING NOTES

The wealth privacy stack is not a luxury. At meaningful wealth levels, it is the difference between being a manageable target and being an easy one.

The structures matter. The infrastructure matters. The operational habits matter. None of them works in isolation. All of them together raise the cost of finding you, watching you, suing you, and attacking you to a level where most adversaries choose easier marks.

The wealthy aren't private because no one knows they exist. They're private because finding them is expensive enough that almost no one bothers. That's the entire game. Every element of this guide is in service of that.

Most HNW individuals are operating with privacy structures that are years out of date and inconsistent with their current wealth level. The gap is the largest it has ever been. Closing it requires building a stack. Building a stack requires expertise, time, and integration across multiple professionals.

The reading of this guide doesn't build the stack. It tells you what good looks like. The next step is yours.