



— BRIEFING / 008 · JULY 2026

DURESS IS A DESIGN PROBLEM.

Ask a principal what their plan is if someone credible threatens their family for a transfer, and the honest answer is usually "I would comply." That is the right answer for the moment and the wrong place to leave the planning. Whether compliance ends the incident safely is decided years earlier, by how the assets were architected. Duress is a design problem, and it can be engineered like one.

EXECUTIVE RISK SERVICES

Prepared for worst-case scenarios. So you don't have to.

info@executiveriskservices.com · referral or invite only

WHY "JUST COMPLY" IS NOT A PLAN

Compliance under coercion is the correct instinct. Nothing held in any wallet is worth a family member's safety, and this series will never suggest otherwise. But compliance only resolves an incident if the principal can actually deliver what is demanded, quickly, and if delivering it plausibly ends the attacker's interest. When everything is reachable in one session, compliance means total loss and no natural endpoint. When nothing is reachable, the principal has no way to de-escalate at all. Both extremes are failures of design, and the principal discovers which one they built only at the worst possible moment.

THE PROPERTY THAT MATTERS: TRUTHFUL DISCLOSURE

The test for duress-resistant architecture is simple to state. Under coercion, the principal must be able to tell the complete truth about how their assets work, comply fully with everything within their power, and still have the structure limit the loss and force time into the incident. Not because the principal is resisting. Because the system was built so that no single person, including its owner, can move everything quickly.

The components are familiar from institutional custody, applied to a personal threat model. A bounded, genuinely accessible layer that can be surrendered immediately and completely, because giving an attacker something real is what de-escalates. Time-delayed movement on everything substantial, disclosed and non-negotiable, so speed is off the table by construction. Approval paths that require parties outside the room, in other places, on other channels, whose involvement is procedural rather than heroic. And no covert tripwires the principal must remember to trigger under stress: the protection has to work when the principal is doing exactly what they are told.

DESIGNING IT BEFORE IT IS NEEDED

None of this can be improvised during an incident, and most of it cannot be retrofitted quickly, which is why it belongs in the same planning cycle as estate work rather than in a crisis response. The design questions a principal and their advisors should be able to answer: What can be moved within one hour by one person under pressure, and is that number an accident or a decision? Which controls

stop working if the principal is coerced rather than hacked? Who outside the household is procedurally required for anything substantial, and do they know what a coerced request looks like? And has the household rehearsed the two sentences that matter, what we hold, and how it moves, so the truth is easy to tell?

Firms in this sector increasingly treat custody design as a personal safety control, not an operational preference. That framing, which Briefing 001 introduced, is the entire point: the architecture is the bodyguard that is always present, cannot be surprised, and does not depend on anyone's courage.

ERS provides executive protection, insider-risk advisory, and custody-governance review for principals in digital assets, finance, and technology. Engagements begin with a conversation: info@executiveriskservices.com.

This briefing discusses duress-resistant design at the level of principle. It deliberately omits protocol specifics, resistance tactics, and anything that would let an attacker calibrate against a real configuration. We publish the pattern and the protective takeaway. We omit operational detail. © 2026 Executive Risk Services, LLC.