



— BRIEFING / 014 · SEPTEMBER 2026

WHEN THE PUBLIC RECORD BECOMES A TARGETING LAYER

New York City published a roll of homeowners, names and addresses included, whose properties may owe a proposed tax on non-primary residences. Within days, digital asset executives were describing it as a target list. Set aside the politics and the merits of the tax. The security question stands on its own, and it is not confined to one city.

EXECUTIVE RISK SERVICES

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

info@executiveriskservices.com · referral or invite only

WHAT WAS RELEASED, AND WHAT WAS NOT NEW

As part of implementing a proposed surcharge on homes that are not the owner's primary residence, New York's Department of Finance published assessment data covering properties that may fall under the new category, with owners' names listed alongside the addresses. The city describes the release as routine and legally required, part of a long tradition of public assessment records that let owners inspect and contest their tax treatment. The file also sweeps broadly: reporting indicates it lists far more properties than will ultimately owe anything, which means many people appear on it who will never be touched by the tax itself.

Property records have been public for a century. Anyone with time and intent could always assemble a picture of who owns what. What changed here is not disclosure but aggregation: a single, cleaned, categorized file that pairs identity with a wealth signal and a residential address, released to everyone at once. That distinction, between data that is technically public and data that is packaged for retrieval, is the entire security story.

52 VERIFIED PHYSICAL ATTACKS ON DIGITAL ASSET HOLDERS WORLDWIDE, H1 2026 (CERTIK)

20 RECORDED HOME INVASIONS IN H1 2026, UP FROM ONE A YEAR EARLIER

88 PEOPLE CHARGED BY FRENCH PROSECUTORS ACROSS A DOZEN CRYPTO KIDNAPPING CASES

WHY AGGREGATION CHANGES EXPOSURE

Targeting begins with research. In every kidnap and extortion pattern ERS tracks, the physical event is preceded by a desk phase: identifying a person of means, connecting them to a location, and building enough of a picture of routine to plan an approach. The cost of that phase is the practical barrier that protects most wealthy people most of the time. Few criminal groups have the patience or capability to do slow, original research.

Aggregated datasets collapse that cost. A file that has already joined name to wealth to address removes the hardest step, and it does so indiscriminately, for every reader at once. This is the same dynamic the digital asset community has lived with on-chain for years: visible wealth invites attention, and the more legible the link between a person and their assets, the more targetable they become in the physical world. The specific file matters less than the direction of travel. Breaches, leaked customer databases, corporate registries, and now official releases keep making hostile research cheaper. Prudent planning treats this as a one-way trend.

— 03 / THE PHYSICAL TREND WAS ALREADY RUNNING

THE PHYSICAL TREND WAS ALREADY RUNNING

This release landed on a community that was already being targeted physically. Blockchain security firm CertiK verified 52 physical coercion attacks against digital asset holders worldwide in the first half of 2026, up from 39 in the same period a year earlier, with estimated financial exposure rising to roughly 124 million dollars. The sharpest movement was in the setting that matters most for families: recorded home invasions rose from one in the first half of 2025 to twenty in the first half of 2026.

Law enforcement activity confirms the pattern is organized rather than opportunistic. French prosecutors have charged 88 people across a dozen kidnapping cases connected to digital asset wealth, and United States federal prosecutors have brought charges in multi-victim robbery and kidnapping cases in California and Minnesota. The consistent thread across jurisdictions is that victims were selected through research, then approached where routine made them predictable: at home and in transit.

— 04 / THE PROTECTIVE READ FOR PRINCIPALS AND FAMILIES

THE PROTECTIVE READ FOR PRINCIPALS AND FAMILIES

The instinctive response to a release like this is anger at the disclosure, followed by an attempt to restore secrecy. Both are understandable, and neither is a plan. The protective conclusions ERS draws for at-risk principals are these.

Assume the address layer is public. Residential security that depends on nobody knowing where you live has already failed. What holds is layered protection at the residence itself: controlled entry, disciplined handling of visitors and deliveries, household staff who are vetted and briefed, and detection that buys time rather than relying on surprise.

Reduce the linkage, not just the listing. Removal from any single dataset has limited value, but the connective tissue between identity, wealth, and location is worth managing deliberately: how properties are titled, what corporate and on-chain footprints reveal, what family members publish, and what staff and vendors can see. The goal is to raise the research cost back up, not to achieve invisibility.

Train the household, not just the principal. Attackers who reach a residence are counting on shock. Families who have rehearsed what an approach looks like, how to respond at the door, in the driveway, and in transit, and who hold a simple standing protocol for the first minutes of an incident behave measurably differently than families improvising under stress. Behavior under pressure is trainable, and it is the variable a family actually controls.

Decide the escalation path in advance. Who is called, in what order, and with what pre-agreed authority. A standing relationship with a response capability is worth more in the first hour of an incident than any amount of improvisation, however well resourced.

— 05 / WHERE PREPARATION FITS

WHERE PREPARATION FITS

ERS delivers kidnap-prevention training for at-risk executives, principals, and their families, built around the pattern described here: the research phase, the approach, and the trained response. It pairs with risk advisory work on footprint reduction and residential security design. The engagements are discreet by design, and they are most valuable before a name appears on any list. For principals whose exposure has changed with this release, the starting point is a conversation about what is currently discoverable and what the household would do tonight if it mattered.

Speak with ERS about kidnap-prevention training

— 06 / SOURCES AND METHOD

SOURCES AND METHOD

This briefing draws on public reporting of the July 2026 New York property roll release, CertiK's H1 2026 wrench attack overview, and published prosecution records in France and the United States. In line with ERS editorial policy, it does not link to or describe how to access the dataset in question, does not name property owners or victims, and discusses protective principles rather than attack methods. That restraint is deliberate: material written to protect principals should never double as material that helps target them.

