— BRIEFING / 021 · SEPTEMBER 2026

ANONYMOUS BY DEFAULT

After its fulfillment partner leaked customer addresses in August, a leading hardware wallet maker announced that its top priority is a delivery option that never learns where its customers live. That decision deserves a closer read than it received.

EXECUTIVE RISK SERVICES

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

info@executiveriskservices.com · referral or invite only

— 01 / THE ANNOUNCEMENT

THE ANNOUNCEMENT

Trezor's August disclosure was, by breach standards, modest: no keys, no funds, roughly 14,000 customers' order details exposed through a logistics vendor. The consequential part came after the apology. The company said its top priority project is establishing an Anonymous Delivery option, a way to buy and receive its products without the company or its vendors retaining the buyer's residential address. In plain terms, a security vendor concluded that knowing where its customers live is a liability to be engineered away rather than a record to be protected harder.

— 02 / WHY THE SHIPPING RECORD IS THE WEAK LINK

WHY THE SHIPPING RECORD IS THE WEAK LINK

Every serious analysis of this year's physical targeting caseload converges on the same input: verified ownership joined to a reachable address. A shipping record for a security product supplies both halves in one row. The buyer has demonstrated they hold assets worth protecting, and the record states where. Firmware can be patched and keys can be rotated; a leaked address cannot be recalled, and past leaks of exactly this data class have fueled extortion campaigns that ran for years. The only address that cannot leak is the one never collected.

— 03 / THE MARKET SIGNAL

THE MARKET SIGNAL

ERS reads the announcement as a leading indicator rather than a one-off. When a vendor makes data non-collection a headline commitment, it is pricing its customers' physical risk into its logistics, and it is betting buyers will choose on that basis. We expect the criterion to spread: security hardware first, then high-end retail categories whose delivery records mark wealth at an address, from watches to firearms accessories to home security equipment itself. Vendors who move early will make it a differentiator. Vendors who lag will make it a disclosure.

— 04 / THE READ FOR PRINCIPALS

THE READ FOR PRINCIPALS

Do not wait for the market to finish the turn. Four habits close most of the gap now. Route security-relevant purchases to an address that is not your residence, through a business, counsel, or a forwarding service. Where lawful and practical, keep the purchasing identity separate from the household. Before buying, ask what the vendor collects, who they share it with, and how long they keep it; the quality of the answer is itself diligence. And commission a periodic review of what past leaks already expose about your addresses, because the record that leaked in 2024 is still working in 2026.

— 05 / THE READ FOR FIRMS

THE READ FOR FIRMS

For companies serving high-net-worth or crypto-holding customers, the lesson generalizes. Every field collected is a field that can leak, and the address field is the one with physical consequences. Data minimization, short retention, and anonymous fulfillment options are no longer privacy niceties. They are safety features, and increasingly they will be judged as such by exactly the customers with the most to lose.

— 06 / SOURCES AND METHOD

SOURCES AND METHOD

This briefing draws on August 2026 disclosure reporting from The Register and industry press. The privacy practices described are lawful, defensive measures for legitimate purchasers. We publish patterns, not workarounds.