— BRIEFING / 020 · SEPTEMBER 2026

THE VENDOR LAYER

In four days this August, three crypto companies disclosed customer data breaches affecting more than a quarter million people. None of the three was breached directly. That is the finding.

EXECUTIVE RISK SERVICES

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

info@executiveriskservices.com · referral or invite only

— 01 / THE CLUSTER

THE CLUSTER

On August 13, hardware wallet maker Trezor disclosed that its fulfillment partner had suffered unauthorized access, exposing the names, email addresses, phone numbers, and shipping addresses of 11,742 customers across seven countries, with a further 1,947 exposed at lesser depth. The company noted it was the first breach in its history to reach customer phone numbers and shipping addresses. On August 16, reporting surfaced a leak at Israel's largest regulated crypto broker said to affect as many as 200,000 customers, including identity documents, bank details, and wallet addresses, the exact file a licensed venue is required to hold. A third disclosure in the same window followed the same third-party pattern, with two of the cluster reportedly traced to the same vulnerability class in a shared analytics platform. Later in the month a Swiss bitcoin broker reported a support-infrastructure exposure affecting several thousand more customers. In every case the intrusion ran through a contracted vendor: fulfillment, analytics, order tracking, support tooling.

3 DISCLOSURES IN FOUR DAYS

253K+ PEOPLE EXPOSED

0 DIRECT INTRUSIONS OF THE NAMED COMPANIES

— 02 / WHAT ACTUALLY LEAKED

WHAT ACTUALLY LEAKED

No private keys were touched and no funds moved. Measured against what these datasets enable, that is limited comfort. A hardware wallet purchase record is a verified statement that a specific person, at a specific address, owns cryptocurrency serious enough to protect. It is not an inference from a marketing list. A KYC file at a regulated broker goes further, pairing that fact with identity documents, banking details, and transaction history. The physical targeting economy documented across this year's caseload runs precisely on this input: confirmed ownership joined to a reachable location. Prior leaks of the same kind have fed multi-year extortion and impersonation campaigns, including demands mailed directly to home addresses.

— 03 / WHY THE VENDOR LAYER

WHY THE VENDOR LAYER

The companies in this cluster invest heavily in securing custody, firmware, and platform. Their vendors do not carry the same posture, and the attackers know it. Fulfillment providers, analytics platforms, and support tools sit outside the hardened core while holding the most physically dangerous data the business touches. The economics favor the attacker at the vendor layer twice over: weaker defenses, and one intrusion yielding many companies' customers when the vendor is shared. This is the same supply chain logic the security industry learned in software, now arriving with physical consequences.

— 04 / THE READ FOR PRINCIPALS

THE READ FOR PRINCIPALS

Assume the pairing of your name and home address with crypto ownership either has leaked or can. Three disciplines reduce the blast radius. Receive security-relevant purchases somewhere other than home, through a forwarding or business address. Where lawful and practical, separate the purchasing identity from the residential one. And periodically commission a check of what existing leaks already say about you, because response beats discovery by the attacker. None of this is exotic; all of it is cheaper than the alternative.

— 05 / THE READ FOR FIRMS

THE READ FOR FIRMS

Vendor diligence in this industry has treated customer PII as a compliance obligation. The 2026 caseload reframes it as a customer safety obligation. Contracts with any vendor holding name and address pairs should carry security requirements, breach notification clocks, and data minimization, and the diligence should ask a blunt question: does this vendor need the data at all, and for how long. The cheapest record to protect is the one never retained.

— 06 / SOURCES AND METHOD

SOURCES AND METHOD

This briefing draws on August 2026 disclosures and reporting from The Block, CoinDesk, The Register, and industry press. We name no affected individuals, omit exploitation details of the shared vulnerability, and reference extortion tactics only at pattern level. The lesson is structural, and it is the structure we publish.