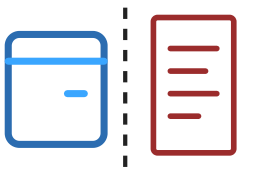
Principal Brief // two-minute read

BREACH & LEAKED DATA | CRYPTOCURRENCY | RESIDENTIAL EXPOSURE

Your Wallet Held. Your Address Did Not.



> *A hardware wallet protects what you own. The order record identifies who you are and where you live, and that record outlived the purchase by six years.*

WHAT HAPPENED

Trezor says an intrusion at its fulfillment provider, ShipMonk, exposed order data for 80,689 customers. Most of that total is roughly 67,000 US orders placed between November 2019 and August 2021, data the provider had repeatedly confirmed in writing was deleted.

WHY IT REACHES YOU

The record holds no recovery phrase, no balance, and no proof you still own the device. It holds your name and delivery address tied to the purchase of a crypto-security product. That is a targeting signal, and it does not expire.

THREE THINGS TO TAKE FROM THIS

1

A purchase is a signal.

The record suggests crypto interest, security awareness, and an asset worth pursuing. The signal is imperfect. Nobody needs certainty to decide who to contact first.

2

Assurance is not deletion.

A retention policy, a contract clause, and a written confirmation are paperwork. Verified destruction is a technical result. Only the last one closes the exposure.

3

The device was never the weak point.

Order, payment, delivery, and support systems keep the identity around a product that is itself well defended. That is where this failed.

DO THIS

- [ ] **YOU, NOW**
  Assume a future message may quote your real order details. Correct details are evidence of the leak, not proof of the sender. Never disclose a recovery phrase or move funds in response to inbound contact.
- [ ] **YOU, WITH YOUR SECURITY LEAD**
  Harden the email account and phone number attached to the order, and require out-of-band verification before any account recovery, security change, or transfer.
- [ ] **YOU AND YOUR HOUSEHOLD**
  Brief family and staff that accurate personal details do not authenticate a caller, a text, or a courier at the door.

NOT THE STORY YOU MAY HAVE HEARD

This was not a compromise of Trezor devices, recovery phrases, wallets, or funds. Replacing a device or moving assets does not retract a leaked name, phone number, email address, or home address.

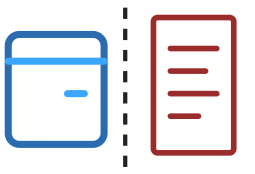
HOW SURE WE ARE

High on the affected population, the exposed fields, and the deletion failure, all from Trezor's own notices. Moderate on the reported technical path, which the provider has not confirmed. No public reporting links this exposure to a physical attack.

THE FULL COMMAND BRIEF FOLLOWS: THE FIVE CONVERSION PATHS, THE COUNTERARGUMENT, AND THE VENDOR TESTS TO RUN.

CB-249

The Wallet Was Secure. The Buyer Was Exposed.



"A secure product still produces an accurate map to the person who bought it."

> *Trezor's devices and wallet infrastructure were not compromised. Its customer relationship was. The distinction matters because an adversary converts identity and delivery data into tailored phishing, account recovery attempts, cross-dataset enrichment, and, in a narrower set of cases, residential targeting.*

BLUF. This is not a cryptocurrency custody failure. It is a principal-exposure failure in the vendor chain. Trezor reports 80,689 customers affected by an intrusion at its fulfillment provider, ShipMonk, and most of that total comes from orders the provider had confirmed in writing were deleted. No keys, recovery seeds, or funds were touched. What escaped is the record of who bought a device built to protect assets, and where it was delivered.

The governing frame: a security-sensitive purchase creates two assets, the product and the record of who acquired it. Organizations defend the first and retain the second. Until verified destruction replaces written assurance, the second asset outlives the transaction and stays available to anyone who reaches the system still holding it.

▶ THE PRACTICAL TEST

Could a stranger use a six-year-old order record to reach you, sound credible, and connect your home to a security-sensitive purchase? If yes, the exposure is real *even though the product remains cryptographically secure.*

THE SIGNAL // WHAT WAS DISCLOSED, AND HOW THE COUNT GREW SIXFOLD

The second disclosure was more consequential than the first, because it surfaced a retention failure rather than only an intrusion.

TREZOR INCIDENT NOTICE · 13 AUG 2026

ShipMonk, a fulfillment provider that packs and ships Trezor orders, notified Trezor on 10 August of unauthorized access to systems holding customer order data. Trezor put the initial population at 13,689 people, 11,742 with full records and 1,947 with partial records, across the US, UK, Sweden, Colombia, Brazil, Italy, and Portugal, for orders received between 10 May and 8 August 2026.

TREZOR INCIDENT UPDATE · 4 SEP 2026

ShipMonk informed Trezor on 2 September that the exposure was larger. Roughly 67,000 additional US customers, from orders placed between November 2019 and August 2021, had full records exposed. Trezor's incident page states a combined total of 80,689 affected customers.

EXPOSED FIELDS · TREZOR NOTICE

Full records carry name, email address, phone number, shipping address, and order number. The partial set carries name, city, and email address. Trezor states that its own systems, devices, wallets, recovery seeds, and funds were not affected.

METABASE ADVISORY 06 AUG 2026 · CISA KEV 11 AUG 2026

CVE-2026-72898 is an unauthenticated SQL injection in the password reset endpoint of Metabase, a business-intelligence tool organizations point at their most complete data stores. Rated CVSS 10.0, it grants administrator access to the instance and to the databases connected to it. Reporting links ShipMonk's exposure to that flaw, and the same window produced disclosures at Framework and Tally. ShipMonk has not publicly acknowledged the incident, and Trezor's notice names no technical path.

ATTRIBUTION · THIRD-PARTY REPORTING

Reporting says ShipMonk received extortion emails from an actor using the ShinyHunters name, and the security firm Halborn attributes the intrusion to that group on pattern analysis rather than direct technical evidence. An extortion contact is not attribution. This brief does not assess the actor as established.

SO WHAT The control that failed first was not access control. It was deletion. A breach can only expose what a system still keeps, and this one kept six-year-old US orders through a 90-day retention policy and repeated written confirmations that they were gone.

THE PRODUCT BOUNDARY // ASSET SECURITY IS NOT PERSON SECURITY

Trezor defended the layer it was built to defend. The layer it lost is the one that concerns a principal, the protected person at the center of a security program. The two are governed by different controls, fail in different ways, and call for different responses, which is why "the devices are secure" is both true and beside the point.

FIGURE 1 // TWO SECURITY LAYERS, ONE TRANSACTION

SECURITY QUESTION	ASSET LAYER	PERSON LAYER
WHAT IS PROTECTED	Private keys, signing, device integrity, recovery material	Name, home, contact channels, relationships, routines
WHAT FAILED HERE	No confirmed failure	Commerce and shipping data escaped the intended boundary
LIKELY ATTACK	Key theft or device compromise	Impersonation, phishing, recovery fraud, coercion, residential focus
USEFUL RESPONSE	Change only on evidence of key or device compromise	Harden identity channels, verification, household posture, data minimization

A secure wallet protects what you own. The receipt helps an adversary decide who to pursue.

WHAT A PURCHASE RECORD PROVES // AND WHAT IT ONLY SUGGESTS

The evidentiary value of a leaked order sits between the two readings now circulating: it is neither proof of wealth nor harmless marketing exhaust. Sorting the inferences by strength is what separates a defensible response from either complacency or alarm.

FIGURE 2 // WHAT THE RECORD SUPPORTS, RANKED BY STRENGTH

INFERENCE	STRENGTH	INTERPRETATION
THE PERSON HAD A RELATIONSHIP WITH TREZOR	High	An order record establishes a historical transaction
THE PERSON HAD AN INTEREST IN CRYPTOCURRENCY SECURITY	Moderate to high	A reasonable inference from the product category
THE PERSON MAY BE WORTH TARGETING	Moderate	The purchase is a prioritization signal, not proof of wealth
THE ADDRESS CAN BE ENRICHED WITH OTHER DATA	High	People-search, property, breach, and social records add context
THE PERSON STILL OWNS THE DEVICE OR HOLDS ASSETS	Not established	The order may be old, gifted, returned, or no longer relevant
THE RECORD REVEALS KEYS, BALANCE, OR RECOVERY PHRASE	No	None of those fields were reported exposed

The practical error is to wait for certainty. An attacker can send one tailored message to an imperfect target at trivial cost, and the cost of being wrong falls entirely on the recipient. A defender therefore treats the record as a credible targeting input without treating all 80,689 people as imminent physical targets.

> **SO WHAT** Your exposure turns less on whether you still own the device than on how easily your name and address join to everything else already published about you.

DELETION BY CONTRACT // THE CONFIRMATION WAS NOT THE CONTROL

Trezor did what a careful counterparty is supposed to do, and it was not enough. It ran a 90-day retention policy for eShop purchase data, imposed a contractual deletion obligation on its provider, and repeatedly requested and received written assurance that the data was gone. The September expansion measures the distance between governance evidence and technical evidence.

FIGURE 3 // FOUR STATES THAT ALL GET CALLED "DELETED"

STATE	WHAT IT MEANS	WHAT IT DOES NOT PROVE
POLICY COMMITMENT	The organization intends to delete on a schedule	That production, analytics, replicas, or backups comply
CONTRACTUAL REQUIREMENT	The vendor is legally obligated to delete	That deletion occurred
WRITTEN CONFIRMATION	The vendor attests that deletion occurred	That every system and recovery path was checked
VERIFIED DESTRUCTION	Evidence ties deletion to defined records and systems	Absolute absence from every undocumented copy

Better deletion assurance is specific. It names the dataset, the identifiers, the systems, the replicas, the treatment of backups, the deletion date, the responsible party, and the validation method. Even then the goal is confidence grounded in evidence, not a ceremonial certificate.

THREAT CONVERSION // FROM ORDER RECORD TO USABLE TARGET

The exposed fields are useful to an attacker in five distinct ways, and only one of them is email phishing. Each path has a control, and the controls are cheap relative to the alternative of responding after contact.

FIGURE 4 // CONVERSION PATHS AND THE CONTROL FOR EACH

PATH	HOW THE EXPOSED DATA HELPS	CONTROL
WALLET-THEMED PHISHING	Correct product and order details make a false alert credible	Navigate independently; never disclose a recovery seed
VOICE OR TEXT IMPERSONATION	Name, phone, and address support urgency and identity theater	Call back through a known channel; use a household safe word
EMAIL ACCOUNT ATTACK	The address identifies the recovery hub for other services	Unique credentials, phishing-resistant MFA, recovery review
CROSS-DATA ENRICHMENT	Address and identity join to property, family, work, or breach records	Reduce broker exposure; audit joined findings, not single records
RESIDENTIAL TARGETING	A delivery address ties a location to a crypto-security purchase	Household briefing, non-residential delivery where lawful, escalation plan

Physical coercion is a real but uneven tail risk, and it is the one path with a documented precedent. Chainalysis recorded 46 publicly reported violent incidents against crypto holders through late June 2026, with home invasions rising to 37 percent of documented cases and relatives or acquaintances targeted in roughly a quarter to a third of them. France accounts for 30 of those incidents, and Chainalysis traces the surge to a 2024 breach in which a French tax official is accused of stealing and selling files on wealthy crypto holders containing names, home addresses, phone numbers, and holdings. Criminal intermediaries are reported to have bought those files and used them to locate targets.

The differences matter as much as the parallel. The French files reportedly carried holdings data, which an order record does not, and no public evidence connects the ShipMonk exposure to a physical incident. What the French case establishes is the mechanism: a list of people who hold cryptocurrency, with addresses attached, has already been converted into physical attacks in another jurisdiction. The data supports preparedness, not alarm.

> **SO WHAT** The people who need this briefing are not only the customer. They are whoever answers the door, the phone, and the email, because the leaked details will sound correct when a caller repeats them.

THE PRECEDENT // THE COMMERCE LAYER HAS FAILED BEFORE

This pattern has now run in public three times in this vendor category. Ledger's 2020 incident exposed roughly one million email addresses and a smaller set of names, postal addresses, phone numbers, and order details, while devices, assets, and payment data were unaffected. In January 2024, Trezor disclosed

a support-portal breach affecting contact data for about 66,000 users, and later warned that some recipients received phishing messages seeking recovery seeds.

The pattern is durable because the incentives are. The cryptographic control holds while customer-service and commerce systems hand an attacker the pretext, the channel, and the target list needed to attack the person around the product.

THE HONEST COUNTERARGUMENT // THE BEST CASE FOR A CALMER READING

THE BEST CASE FOR THE OTHER SIDE

+ No keys, seeds, or funds were exposed, and Trezor's own systems were not breached. The product did the job it was sold to do.
+ Much of the exposed data is old. An order from 2019 says little reliable about who lives at that address in 2026, whether the device was kept, or whether the buyer holds anything worth taking.
+ Trezor was not negligent by ordinary standards. It set a retention policy, contracted for deletion, and asked for written confirmation. The failure was its provider's.
+ Forty-six violent incidents worldwide in six months is a very small number set against a population of 80,689, and no public reporting ties this exposure to any of them.
+ Treating every affected customer as a target produces alert fatigue, which is itself a security cost.

All of that is true, and none of it reaches the finding. Cost asymmetry does: an attacker can act on a weak signal for the price of one message, while a defender who waits for certainty acts only after contact has already been made. The negligence question is also beside the point for a principal, who inherits the consequence of a vendor's retention practice regardless of whose contract failed. The lesson is not that Trezor erred. It is that written assurance is not a control.

THE CONTROL MAP // PROTECT THE TRANSACTION AROUND THE PRODUCT

Reducing this exposure means changing how a security-sensitive purchase is made, not which wallet is chosen. Each surface below is set at purchase time, which is why the remedy is prospective rather than reactive.

FIGURE 5 // SURFACES SET AT PURCHASE TIME, AND THE BETTER POSTURE FOR EACH

SURFACE	BETTER POSTURE
DELIVERY IDENTITY	Use the least identifying lawful delivery option; avoid a principal's residence where operationally appropriate
CONTACT CHANNELS	Segment security-sensitive purchases from public and recovery identities
PAYMENT TRAIL	Assume payment creates metadata; cryptocurrency payment is not automatically anonymous
VENDOR RETENTION	Map processors, carriers, support systems, analytics stores, exports, and backups; test deletion evidence
HOUSEHOLD VERIFICATION	Train family and staff to distrust inbound urgency, even when the sender knows accurate details
RESIDENTIAL EXPOSURE	Review public links between principal, property, family, vehicles, and routines

Trezor says its planned Anonymous Delivery model will use locker collection, neutral packaging, a generic sender, and automatic deletion of identifying information, with EU rollout in September 2026 and US expansion expected by year end. The direction is sound. Its practical privacy will depend on what identity and transaction metadata survives across payment, fulfillment, carrier, locker, notification, fraud, and support systems, which is precisely the layer that failed here.

ASSESSMENT

FIGURE 6 // ANALYTIC CONFIDENCE BY CLAIM

Trezor reports 80,689 affected customers, most of them from orders the provider had confirmed were deleted.	**STRONG / VENDOR-CONFIRMED**
Devices, wallets, recovery seeds, and customer funds were not compromised.	**STRONG / VENDOR-CONFIRMED**
The exposed fields materially improve phishing, impersonation, and account-recovery attacks.	**STRONG / REPLICATED**
Written deletion confirmation is administrative evidence and does not establish that data was destroyed.	**STRONG / DEMONSTRATED HERE**
The records can support residential targeting once joined to other data about the same person.	**MODERATE / NO LINKED INCIDENT**
CVE-2026-72898 in Metabase was the intrusion path into the provider.	**MODERATE / PROVIDER-UNCONFIRMED**
ShinyHunters conducted the intrusion.	NOT ESTABLISHED / ATTRIBUTION BY PATTERN
An order record shows current device ownership, holdings, or wealth.	REJECTED / NOT SUPPORTED
Replacing the device or moving funds resolves the exposure.	REJECTED / WRONG LAYER

Risk is not equal across the affected population. Public prominence, property visibility, family exposure, and the density of already-published data about a person determine whether a record converts into anything at all.

POSTURE

FOR PRINCIPALS

- → Assume any future message may quote real order details, and treat correct details as evidence of the leak rather than proof of the sender.
- → Never disclose a recovery seed, approve an unsolicited security change, or move assets in response to inbound contact.
- → Harden the email account and phone number attached to the order, since that address is the recovery hub for much else.
- → Do not replace a wallet or move funds solely because of this notice; change devices on evidence of key or device compromise, not on notification.

FOR FAMILY OFFICES

- → Treat wallet, exchange, tax, payment, support, and delivery records as one exposure graph rather than separate vendor relationships.
- → Segment contact and delivery channels so a security-sensitive purchase does not resolve to a principal's residence.
- → Brief family and staff on inbound urgency, and set a household verification word that no vendor record can supply.
- → Existing ObscureIQ clients should add the affected population to the next exposure-audit cycle, so new joins carrying residential and relationship data are assessed.

FOR SECURITY & LEGAL FUNCTIONS

- → Classify vendors by what their records imply, not only by regulated field type. An order record is not regulated data and is high-value targeting data.
- → Require deletion obligations that name systems, replicas, backups, evidence, and a validation method, then test them against expired records, analytics copies, export folders, and restore paths.
- → Inventory internet-reachable business-intelligence tooling across the vendor chain; that layer holds the join, not a slice.
- → Build incident playbooks for data that raises physical or coercive risk without containing a credential. This is analysis, not legal advice.

CONFIDENCE High on the affected population, the exposed fields, the retention failure, and the absence of key or fund compromise, all of which rest on Trezor's own notices. Moderate on the Metabase intrusion path, which is well supported by the vendor advisory, the CISA catalog entry, and multiple outlets, but is not confirmed by the fulfillment provider and is not named in Trezor's notice. Moderate on residential targeting potential, which follows from data composition and an external threat pattern with no incident yet linked to this exposure. The actor is not assessed as established.

METHOD Vendor-confirmed facts are separated from third-party reporting and from analytical inference, and every claim in Figure 6 carries its basis. The wrench-attack record is treated as context for conversion potential, not as evidence about this incident. Cross-read against ObscureIQ doctrine on breach exposure states, notification, and destruction.

SOURCES Trezor, Recent customer data exposed in shipping provider incident (13 Aug and 4 Sep 2026); The Hacker News, Metabase zero-day exploited in the wild (12 Aug 2026); Ledger, Addressing the July 2020 e-commerce and marketing data breach; Chainalysis, Violent wrench attacks targeting crypto holders (6 Aug 2026). Context: BleepingComputer, Trezor data breach impact now reaches 81,000 customers; Halborn, Explained: the Trezor/ShipMonk breach.

Scope note: population and field figures come from Trezor's notices and should be confirmed against the vendor page before external reproduction; at least one outlet has noted that row-level overlap between the two disclosed groups is not public. Violent-incident counts differ by publisher and verification standard, with Chainalysis recording 46 incidents through late June 2026 and CertiK verifying 52 for the first half of the year; neither is a base rate for this population. Vendor and security-firm statements are attributed, not asserted. This is intelligence analysis, not legal advice.

OBSCUREIQ INTERNAL ANALYSIS // ARCHIVE COMM-249-VENDOR-CHAIN-PURCHASE-EXPOSURE-2026Q3 // XREF **CB-230 CB-231 CB-247** // ACCESS PUBLIC · OPEN TO ALL READERS ON RELEASE