

Forum: [Hack Forums](#)

Thread: [Trezor data breach](#)

Yin Yang - August 13, 2026, 1:21 pm

Yikes

Quote: ShipMonk, Trezor's fulfillment partner, suffered unauthorized access to its systems, affecting nearly 14,000 customers' data, the cold storage crypto wallet firm reported Thursday.

MadScientist - August 13, 2026, 1:44 pm

Wonder what data, haven't check but, prepare the floodgates for targeted spear fishing and simswaps

Yin Yang - August 13, 2026, 5:20 pm

(Aug 13, 2026 01:44 PM)MadScientist Wrote: [\[CITE\]](#) Wonder what data, haven't check but, prepare the floodgates for targeted spear fishing and simswaps Oh 100%. Name, physical address where it was shipped and email

SIM-1169085 - August 13, 2026, 5:32 pm

Bought mine years ago so I guess I'm safe. This happened to Ledger years ago and I'm still getting emails from these yahoos.

We're gonna be seeing a lot of hardware wallet news since cold card wallets hack was broadcasted so recently.

Mewtwo - August 13, 2026, 5:34 pm

Bought my new Trezor like 2 weeks ago. Not so happy about this. I used a disposable email, but my address is ofc real. Come rob me, I'll fucking shoot ya

MadScientist - August 13, 2026, 5:35 pm

(Aug 13, 2026 05:34 PM)Mewtwo Wrote: [\[CITE\]](#) Bought my new Trezor like 2 weeks ago. Not so happy about this. I used a disposable email, but my address is ofc real. Come rob me, I'll fucking shoot ya

I'm already in your closet ?

Money- - August 13, 2026, 9:26 pm

(Aug 13, 2026 05:34 PM)Mewtwo Wrote: [\[CITE\]](#) Bought my new Trezor like 2 weeks ago. Not so happy about this. I used a disposable email, but my address is ofc real. Come rob me, I'll fucking shoot ya

I'll see you bro. I am gona use a different way.

Omniscient - August 14, 2026, 10:32 am

Likely an increase is exploit spam and phishing attempts because of this. I kind of doubt simswapping and kidnapping will be prevalent. Not without someone obviously bragging about having millions in crypto.

A lot of people have hardware wallets for only \$1-10k in funds.

SUI-3183372 - August 14, 2026, 11:23 am

After Ledger's breach, some people were receiving 20-30 scam calls per day, at all hours of the day.

There was a case where one of these individuals was a MD who would be on call over night, unable to shut his phone off nor could he ignore phone calls. Blocking numbers / spam filtering is only so effective. Eventually he had to change all of his info because the scam calls were so pervasive.

I have colleagues who, to this day, receiving physical scam mail on a regular basis.

In some cases, scammers have sent new Ledgers to victim addresses. Scammers will buy new ledgers, pre-load a seed phrase onto it, fabricate a new instruction manual that makes it seem like a pre-loaded wallet is normal, and fabricate written correspondence "from Ledger" that explains that the old device that the victim had bought was faulty and Ledger was sending them a brand new replacement device, and to move funds to the new device. Anyone who did so, trusting the pre-loaded wallet (which was a non-zero number of people), got owned immediately.

Scammers have been very persistent and sometimes quite clever with the leaked Ledger data. Now that have a brand new cache of names and addresses that they can double their efforts down on. Annoying day for those impacted, hopefully no physical attacks stem from this.

If you live in France and are part of this leak... consider moving anywhere else... There have been 54 recorded instances of physical attacks and kidnappings related to crypto globally so far this year. 34 of those instances (63%) have occurred in France.

Omniscient - August 15, 2026, 12:38 pm

(Aug 14, 2026 11:23 AM)SUI-3183372 Wrote: [CITE](#) After Ledger's breach, some people were receiving 20-30 scam calls per day, at all hours of the day.

There was a case where one of these individuals was a MD who would be on call over night, unable to shut his phone off nor could he ignore phone calls. Blocking numbers / spam filtering is only so effective. Eventually he had to change all of his info because the scam calls were so pervasive.

I have colleagues who, to this day, receiving physical scam mail on a regular basis.

In some cases, scammers have sent new Ledgers to victim addresses. Scammers will buy new ledgers, pre-load a seed phrase onto it, fabricate a new instruction manual that makes it seem like a pre-loaded wallet is normal, and fabricate written correspondence "from Ledger" that explains that the old device that the victim had bought was faulty and Ledger was sending them a brand new replacement device, and to move funds to the new device. Anyone who did so, trusting the pre-loaded wallet (which was a non-zero number of people), got owned immediately.

Scammers have been very persistent and sometimes quite clever with the leaked Ledger data. Now that have a brand new cache of names and addresses that they can double their efforts down on. Annoying day for those impacted, hopefully no physical attacks stem from this.

If you live in France and are part of this leak... consider moving anywhere else... There have been 54 recorded instances of physical attacks and kidnappings related to crypto globally so far this year. 34 of those instances (63%) have occurred in France.

Crazy scenarios some of which I hadn't heard about yet. Like the pre-loaded Ledger wallets. Nuts.

Where there is money, there are scams.

SUI-3183372 - August 16, 2026, 8:27 am

Another hardware wallet has leaked payment/shipping data to unauthorized third parties:

Quote:The incident impacts approximately 39,798 customers who placed orders between March 2, 2025 and April 11, 2026. Exposed information includes name, email address, shipping address, phone number, and purchase details.

jcole - August 24, 2026, 2:31 pm

Luckily I bought my Trezor before there was a broadcasted data leak.

Cap - September 5, 2026, 5:38 pm

(Aug 14, 2026 11:23 AM)SUI-3183372 Wrote: [\[CITE\]](#) After Ledger's breach, some people were receiving 20-30 scam calls per day, at all hours of the day.

There was a case where one of these individuals was a MD who would be on call over night, unable to shut his phone off nor could he ignore phone calls. Blocking numbers / spam filtering is only so effective. Eventually he had to change all of his info because the scam calls were so pervasive.

I have colleagues who, to this day, receiving physical scam mail on a regular basis.

In some cases, scammers have sent new Ledgers to victim addresses. Scammers will buy new ledgers, pre-load a seed phrase onto it, fabricate a new instruction manual that makes it seem like a pre-loaded wallet is normal, and fabricate written correspondence "from Ledger" that explains that the old device that the victim had bought was faulty and Ledger was sending them a brand new replacement device, and to move funds to the new device. Anyone who did so, trusting the pre-loaded wallet (which was a non-zero number of people), got owned immediately.

Scammers have been very persistent and sometimes quite clever with the leaked Ledger data. Now that have a brand new cache of names and addresses that they can double their efforts down on. Annoying day for those impacted, hopefully no physical attacks stem from this.

If you live in France and are part of this leak... consider moving anywhere else... There have been 54 recorded instances of physical attacks and kidnappings related to crypto globally so far this year. 34 of those instances (63%) have occurred in France.

I actually just received physical mail the other day for the Trezor breach saying they'll be sending me a new Trezor within the next week or so. They also have a QR code to scan to see if my current hardware wallet was affected.

Omniscient - September 7, 2026, 12:16 pm

(Sep 5, 2026 05:38 PM)Cap Wrote: [\[CITE\]](#) I actually just received physical mail the other day for the Trezor breach saying they'll be sending me a new Trezor within the next week or so. They also have a QR code to scan to see if my current hardware wallet was affected.

Ugh, that sounds like the scam [SUI-3183372](#) described. You may want to read his posts in this thread again.

I don't see how the data breach forces them to send you a new Trezor. It changes nothing for your security. Be super careful.

Cap - September 7, 2026, 1:38 pm

(Sep 7, 2026 12:16 PM)Omniscient Wrote: [\[CITE\]](#) Ugh, that sounds like the scam [SUI-3183372](#) described. You may want to read his posts in this thread again.

I don't see how the data breach forces them to send you a new Trezor. It changes nothing for your security. Be super careful.

Yeah, super strange scam. Like you said, I don't know how getting a new Trezor would increase the security if it was a data breach. Definitely going to be careful.

SUI-3183372 - September 7, 2026, 4:06 pm

(Sep 7, 2026 01:38 PM)Cap Wrote: [\[CITE\]](#) Yeah, super strange scam. Like you said, I don't know how getting a new Trezor would increase the security if it was a data breach. Definitely going to be careful.

Yep, your current device is just fine. Make no changes.

This new device will likely be tampered with, either they'll try to convince you to trust a pre-loaded seed phrase, or potentially a more complex approach.

Security Alliance/SEAL911 would likely be interested in collaborating with you to learn more about the devices that scammers are dispatching.

SUI-3183372 - September 8, 2026, 4:52 pm

Larger impact landscape than previously disclosed:

Mewtwo - September 9, 2026, 12:46 am

(Sep 8, 2026 04:52 PM)SUI-3183372 Wrote: [\[CITE\]](#) Larger impact landscape than previously disclosed:

Class action lawsuit pls. I want my \$10

SUI-3183372 - September 9, 2026, 8:24 am

(Sep 9, 2026 12:46 AM)Mewtwo Wrote: [\[CITE\]](#) Class action lawsuit pls. I want my \$10

Seems pretty open and shut. Initially, ShipMonk was assuring Trezor that they were deleting customer data at Trezor's request. ShipMonk were lying.

Then, overtime, ShipMonk became contractually obligated to manage this data in a certain manner (do not store). ShipMonk breached this contract, never followed it.

You'd think that Trezor have a real easy open and shut case against ShipMonk. You'd think that Trezor would be up in arms after being blatantly lied to for years. Yet Trezor aren't going to do shit, Trezor are pointing their finger at ShipMonk then deflecting questions around "so what are you going to do about it?"

Trezor is likely complicit, the requests and/or contracts likely didn't exist or Trezor knew they weren't being followed. Their inaction despite knowing this takes away their teeth.

Omniscient - September 9, 2026, 2:37 pm

(Sep 9, 2026 08:24 AM)SUI-3183372 Wrote: [\[CITE\]](#) Seems pretty open and shut. Initially, ShipMonk was assuring Trezor that they were deleting customer data at Trezor's request. ShipMonk were lying.

Then, overtime, ShipMonk became contractually obligated to manage this data in a certain manner (do not store). ShipMonk breached this contract, never followed it.

You'd think that Trezor have a real easy open and shut case against ShipMonk. You'd think that Trezor would be up in arms after being blatantly lied to for years. Yet Trezor aren't going to do shit, Trezor are pointing their finger at ShipMonk then deflecting questions around "so what are you going to do about it?"

Trezor is likely complicit, the requests and/or contracts likely didn't exist or Trezor knew they weren't being followed. Their inaction despite knowing this takes away their teeth.

But I wonder how effective suing in certain countries really is. In America we sue for everything. Results may vary greatly in their country, making it not worth it.

SUI-3183372 - September 9, 2026, 2:52 pm

(Sep 9, 2026 02:37 PM)Omniscient Wrote: [\[CITE\]](#) But I wonder how effective suing in certain countries really is. In America we sue for everything. Results may vary greatly in their country, making it not worth it.

Both Trezor and ShipMonk are based out of Czech Republic, so it simplifies things a bit. Unsure how Czech courts operate, but they're still an EU country, I'd imagine breach of contract and mismanagement of sensitive data has to hold some sort of weight.