Yoroi / SecondFi Wallet Incident — On-Chain Analysis

Snapshot as of: 24 June 2026, ~10:54 UTC — active, evolving incident; figures may change. **Status:** Independently verified on-chain (Blockfrost + Cardano node data) unless marked as a community estimate or attributed to SecondFi. *(All USD figures use ADA ≈ $0.15.)*

TL;DR

- A mass wallet compromise has affected Cardano users of **Yoroi / SecondFi**. Per SecondFi, the incident comprises **4 draining events**.
- **External theft:** SecondFi has acknowledged **~16M ADA stolen across 374 addresses** by external threat actors (3 of the 4 events). We have **independently mapped ~12.1M ADA across ~178 wallets** — one of those events (fee-sponsored drainer → collectors A/B/C → DEX laundering). The remaining ~2 events (~4M / ~196 addresses) are **not yet independently mapped**.
- **The ~129M "Wave 2":** SecondFi states this was **their own emergency white-hat rescue** — sweeping ~129.43M ADA from ~2,850 at-risk (largely whale) wallets to secure them, to be routed to a third-party custodian and returned to affected users.
- **On-chain caveat on the rescue:** as of this snapshot the ~129.43M **remains in a single wallet, unmoved since 23 Jun 12:20 UTC** — **no transfer to any custodian has been observed on-chain yet**, and no custodian or audit firm has been publicly named. The behaviour (held, never laundered, never sent to an exchange) is **consistent with** a rescue/hold; independent confirmation awaits the custodian transfer.
- **Mechanism:** drains were signed using the **affected wallets' own keys** — a key-compromise event, **not** a Cardano protocol or smart-contract exploit.
- **The Cardano network is safe** — no protocol compromise or chain reorganisation has been observed.

What SecondFi has officially acknowledged

From SecondFi (@secondfiapp) on 23–24 June 2026:

- **4 distinct draining events.** 3 were by **external threat actors**, totalling **~16M ADA across 374 addresses**.
- To prevent further loss during the active exploit, SecondFi says it triggered **emergency rescue measures to secure ~129M ADA**, which "continues to be routed to an independent, qualified third-party custodian… held securely for the benefit of the affected wallet addresses," with an external accounting firm engaged for a special audit.
- Root cause identified as **"at the address level"** — the risk triggers "when an affected user signs a transaction." A patch has been rolled out for unaffected wallets.
- Affected users are directed to claim via **support.secondfi.io**.

SecondFi statement timeline (UTC):

- 23 Jun ~06:26 — "security issue… paused affected functions… maintenance mode."
- 23 Jun ~11:21 — estimates total impact "approximately 16M ADA"; says "extraordinary steps to protect remaining assets" were taken.
- 24 Jun ~05:40 — root cause "at the address level"; advises against restoring the recovery phrase; "we have isolated the affected wallets."
- 24 Jun ~09:47 — the 4-events breakdown: ~16M / 374 stolen by external actors; ~129M secured by emergency rescue and "being routed to a third-party custodian"; external audit engaged; patch rolled out.

This document reports what is independently verifiable on-chain, and clearly separates that from SecondFi's stated account.

The two components, side by side

	External theft	**SecondFi emergency rescue**
Nature	Criminal theft by external actors	White-hat sweep by SecondFi (per their statement)
ADA	**~16M total (SecondFi) · ~12.1M independently mapped**	**~129.43M**
Addresses	**374 (SecondFi) · ~178 mapped**	**~2,850**
Events	3 (we mapped 1)	1
Method	Fee-sponsored sweeps (NEAR-bridge funding → fee-sponsor → collectors A/B/C)	Key-compromise sweep, consolidated into one wallet
Status of funds	Laundered / dispersed via DEX pools (incl. an ADA→USDCx dump that spiked the USDCx pair)	Parked in a single wallet; SecondFi says being routed to a custodian — **not yet observed on-chain**
Biggest single wallet	3.30M ADA (stolen)	5.41M ADA (rescued)

USD at ADA ≈ $0.15: ~16M ≈ $2.4M stolen; ~129.43M ≈ $19.4M rescued/held.

---

1. The external theft — what we independently mapped (~12.1M / ~178)

This is one of SecondFi's three external events, fully traced on-chain:

```
NEAR Intents bridge treasury (addr1v8wfp…)   ← fresh, no-KYC ADA
        ▼
Fee-sponsor wallet (addr1q8acx…)  ← born 21 Jun 15:17; paid gas for ~196 sweeps
        ▼
~178 victim wallets ─► 3 collectors A/B/C (5.68M / 3.36M / 3.15M) = ~12.1M ADA
        ▼
Smart-contract cluster (stake1u9fg8znea…)  → DEX-pool token→ADA laundering
```

- Verified: **12,108,954 ADA from 192 addresses (~178 wallets)**, window 21 Jun 20:29 → 22 Jun 00:35 UTC.
- The drains were **signed by each victim wallet's own key** (every victim address is a key-based address, so Cardano's ledger required a valid signature to move the funds — this is provable, not inferred).
- The attackers then **dumped ~1.12M ADA into USDCx** (spiking the ADA/USDCx pair on 21 Jun) and routed proceeds through DEX pools — confirming the theft was being actively liquidated.
- Multiple victims have publicly named collectors **B** and **C** as the wallets that drained them.

Biggest mapped victims: 3.30M · 1.54M · 1.32M · 1.09M ADA (4 wallets >1M); 13 lost 100k–1M; 41 lost 10k–100k; 57 lost 1k–10k; 77 lost <1k.

The remaining ~4M / ~196 addresses (SecondFi's other 2 external events) are not yet independently mapped — neither by us nor, per community trackers, publicly. We cite SecondFi's ~16M / 374 figure for the full external total.

---

2. The ~129M — SecondFi's stated emergency rescue ("Wave 2")

- SecondFi states it swept **~129.43M ADA from ~2,850 at-risk wallets** to secure them during the active exploit.
- On-chain, the sweep ran **23 Jun 03:00–09:00 UTC** (~2,855 transactions, peak 1,948 in the 07:00 hour), pulling ADA **plus tokens and NFTs — including 252 users' ADA Handles** — from ~2,850 wallets (each emptied to zero). The funds were then consolidated into a single wallet (`addr1qxd39k4…`) on 23 June via two 60M transfers plus smaller mop-ups (11:19–12:20 UTC), and have **sat there untouched since 12:20 UTC on 23 June**.
- The ~2,850 rescued wallets are **whale-skewed**: 27 lost-and-secured >1M ADA each (largest 5.41M).

What is verifiable vs. stated:

- ✅ Verifiable on-chain: ~129.43M is consolidated in one wallet, has **never been laundered or sent to any exchange/DEX/bridge**, and remains parked.
- ⚠️ Stated by SecondFi, **not yet visible on-chain:** that it is "being routed to a third-party custodian." As of 24 Jun 10:54 UTC **no custodian transfer has occurred** and no custodian/auditor has been named. The funds simply remain in the one wallet.

The held-and-unlaundered behaviour is consistent with a rescue/custody hold rather than a theft (a thief liquidates; this wallet has not). Full independent confirmation will come when/if the funds move to a named, audited custodian — which we are monitoring for.

---

3. Mechanism & root cause

- **Mechanism (confirmed on-chain):** funds moved via transactions **signed by the affected wallets' own keys** (each victim address is key-based, so a valid signature was mandatory under Cardano's rules). The same signing capability appears to underlie both the external theft and SecondFi's rescue sweep.
- **Root cause (not determinable from chain data):** SecondFi says it is "at the address level," triggered when an affected user signs a transaction. On-chain evidence shows *that* keys/signing were compromised and *where* funds went — not *how*. Treat any specific root-cause claim as unconfirmed pending an official post-mortem.

---

4. Live status (24 Jun ~10:54 UTC)

- **SecondFi rescue (~129.43M):** parked in `addr1qxd39k4…`, unmoved since 23 Jun 12:20 UTC; no custodian transfer observed.
- **External theft (~12.1M mapped):** laundered/dispersed through DEX pools; collector wallets emptied.
- **Sweeping tail still ongoing:** a trickle of smaller wallets continued to be swept into the collection wallet (most recent observed 24 Jun ~10:05 UTC).
- A live monitor is watching the key wallets for any movement (custodian transfer or onward laundering).

---

5. If you used Yoroi / SecondFi

1. **Assume your wallet is compromised.** Treat the seed phrase / keys as exposed.
2. **Beware impersonators.** A real team will **never** DM you first, ask for your seed phrase, or ask you to "validate"/move funds. Ignore unsolicited "support" DMs.
3. **Follow official channels only.** Watch SecondFi's verified account and support.secondfi.io for updates, and verify anything claiming to be "official steps" is from the genuine verified source.
4. **Preserve evidence:** your wallet address, the drain transaction hash, amounts, and timestamps.

---

6. Verify this yourself

Every figure here is on-chain and public. Paste any address into a Cardano explorer (cexplorer.io, adastat.net):

- SecondFi rescue wallet (~129.43M, parked): `addr1qxd39k4peszxlf0x59e88hngpe5u9882y2lyhdzazsq4kfvmztd2rnqyd7j7dgtjw00xsrnfc2ww5g47fw6969qptvjshwxpl3`
- External-theft collector (community-named by victims): `addr1q82jlp2u0ezv2hsf6f40fkrv49hd72yv442nmrr5qeultpqamepaykp3m564hnd4zp75wxxds2j6d3ywvc8prhf2kcxqn6nql3`

---

7. Address & transaction reference

Role	Address
SecondFi rescue wallet (holds ~129.43M)	`addr1qxd39k4peszxlf0x59e88hngpe5u9882y2lyhdzazsq4kfvmztd2rnqyd7j7dgtjw00xsrnfc2ww5g47fw6969qptvjshwxpl3`
Rescue collection wallet (pre-consolidation)	`addr1q8g8cgwqw98q2mrzrwgcy3wectdxwem8a8zp9r2mn6wjy7q4x7gcpv39wwurj7n72akw4kd0dgmv72gz4j92fvhn29ss7vuz99`
External-theft fee sponsor	`addr1q8acx4h5a38x6ekpsp0x7aelw6mflt78khmz8lz75rtnqvn07w88zx2e89tgzqr3x0mecngqlg87kq9surhk48hj79mqcezfa8`
Fee-sponsor stake key	`stake1u9hl8rn3r9vnj45pqpcn8auuf5q05rltqzcwpmm2nme0zasf40ymg`

Role	Address
Fee-sponsor funding (NEAR Intents bridge)	`addr1v8wfpcg4qfhmnzprzysj6j9c53u5j56j8rvhyjp08s53s6g07rfjm`
Theft collector A	`addr1q9j7f598x988unr4zhjulft205jqnn9ewgwkhes5smf2sr6jsw98nm4qq38jw9epe587twavuhuhj5d8r92rjvmyjlzs9lqc3x`
Theft collector B	`addr1q82jlp2u0ezv2hsf6f40fkrv49hd72yv442nmrr5qeultpqamepaykp3m564hnd4zp75wxxds2j6d3ywvc8prhf2kcxqn6nql3`
Theft collector B stake key	`stake1uywaus7jtqca6d2mek63ql28rrxc9fdxcj8xvrs3m54tvrq4uaarv`
Theft collector C	`addr1q9wudkfeelzwev427yvapkmqexmet8q4vl303m7a4eerwtvt6rq00zyuqzeuw759vgqtdky0gyxnqx27n8q4k6h79yhsqelma8`
Theft collector C stake key	`stake1ux9aps8h3zwqpv7802zkyq9kmz85zrfsr90fns2mdtlzjtcm7jj8p`
Theft accumulation / laundering stake key	`stake1u9fg8znea6sqgne8zusu6rl9hwkwt7te2xn3j4pexdjf03g4kw9uq`
USDCx laundering hub	`addr1q8nw4dkulh8w5gdst5q87pdq9kkdpvvxpqta37qx6maryrkelj2ugdyg7kyc7xuleagy883fdtxqywym02ty3luptv9qhl98qc`

Transaction hashes: fee-sponsor split `c2301f306dd1b2f802b11e92bd3efbf727d348d9ce5683e78739b23137cc97e1` ; funder→fee-sponsor `857187f7e9bb495f4d8531bfe004744af160f44cad3aaef70b69dbd38897d37f` , `808d9a0cacc5ded5c17fd2930366144ded4eb71642ff07218eff4a32c677904b` ; victim drain (partial) `16f81996…08814` .

---

8. Methodology

- On-chain data pulled directly from a Cardano mainnet node via Blockfrost: balances/totals, full UTxO sets, per-transaction input/output graphs, wallet ages, and stake clustering.
- The external theft was reconstructed by enumerating every sweep transaction the fee-sponsor co-signed, confirming each victim was emptied and signed/paid its own fee, and aggregating per-victim losses.
- Cross-checked against an independent DEX-swap index (16 Cardano DEXes) to confirm the laundering route, and against community/on-chain-investigator reporting.
- SecondFi's figures (~16M / 374; the ~129M rescue) are reported as their stated account; we flag explicitly where on-chain evidence does not yet corroborate them (e.g. the custodian transfer).

---

*Disclaimer: Preliminary technical analysis based on public on-chain data, published for the protection of affected users and to assist investigators. It does **not** allege wrongdoing by SecondFi, Emurgo, any exchange, bridge, or other third party. On-chain data shows where funds moved and that signing was compromised — not how; root cause is unconfirmed pending an official post-mortem. SecondFi's rescue/custodian statements are reported as their account and, where noted, are not yet independently verifiable on-chain. Figures are a point-in-time snapshot and may change. Not financial or legal advice. Compiled by Fetch — Cardano DEX Aggregator (cardano.fetchswap.io).*