

Evidence Report: Money Trail & IC3 Filing Text

Prepared for: EXAMPLE CUSTOMER · **Your wallet:** EXAMPLE wallet (see IC3 text) · **Prepared:** Oct 2026 · **Delivery:** within 24 hours

SAMPLE: EXAMPLE DATA ONLY. This is a made-up case. The wallets, transaction IDs, amounts and times are invented to show what this report looks like. They are not real victims or real wallets. Do not file anything from this sample.

SAMPLE: made-up example case for illustration. Amounts and times are invented.

This report is for you to file yourself. Nothing has been sent or posted for you. Filing with the FBI's IC3 is free, and there is no minimum loss. Take screenshots of any posts, chats or sites you remember before you file, because they often get deleted.

Never share your seed phrase or private key with anyone. WalletTies will never ask for it, never DMs first, and never asks you to connect your wallet. IC3 will never contact you to ask for money. Anyone offering to "recover" your crypto for a fee is almost certainly running a second scam.

What went into this report

Transaction signatures scanned	4,812
Transactions fetched and analyzed	1,036
Wallets examined (cap about 40)	38
Hops traced (up to 5, 3 biggest branches)	4
Exchange-labeled deposit addresses	1
Human review	about 20 minutes

Example numbers for this made-up sample.

What happened to you, in plain English

On Mar 3, 2026 someone you met in a Telegram trading group convinced you to send 42 SOL (about \$6,300) to a "staking vault" that promised 3% a day. The vault address was an ordinary wallet. Within 40 minutes your SOL was moved through a short-lived wallet, swapped to USDC, and most of it (about 6,050 USDC) appears to have landed in a deposit address at a large exchange. That exchange deposit is the most useful lead in this report: exchanges can identify their customers when law enforcement asks.

This isn't your fault

These scams are built to fool careful people, and they happen constantly. The FBI's IC3 received 181,565 complaints involving cryptocurrency in 2025. By filing, you're doing something real: IC3 says its data is most useful when complaints are combined, because that lets the FBI connect cases. We can't promise you'll get money back. Nobody honest can. But your report counts.

1. Summary

Scam type	Fake staking / investment (appears to be)
You sent	about 42 SOL (about \$6,300) on Mar 3, 2026
Where it appears to have gone	Exchange-labeled deposit address (hop 4)
Best next step	File with FBI IC3 (free) and paste the text in section 3

2. Money trail (hop by hop)

#	Time	From	To	Amount	TX	Appears to be
1	Mar 3, 2026 9:12 PM ET	EXAMPL...zVqd	EXAMPL...Q59r	42.0 SOL	EXAMPL...raYP	"Staking vault"
2	Mar 3, 2026 9:20 PM ET	EXAMPL...Q59r	EXAMPL...6r8R	41.9 SOL	EXAMPL...LyCS	Intermediate
3	Mar 3, 2026 9:31 PM ET	EXAMPL...6r8R	EXAMPL...Zbz2	41.9 SOL to 6,061 USDC	EXAMPL...YasJ	Swap
4	Mar 3, 2026 9:52 PM ET	EXAMPL...Zbz2	EXAMPL...1bYm	6,050 USDC	EXAMPL...v2zA	Exchange deposit (labeled)

Addresses and TX IDs are shortened in this table; the full values are in the IC3 complaint text below. Each hop can be checked on a public Solana explorer. "Appears to be" labels are inferences from on-chain patterns, not proven identities.

3. IC3 complaint text: copy and paste into the IC3 form

IC3 doesn't accept attachments, so this section is plain text made for pasting. Paste the text into the IC3 form and keep this PDF in case an investigator asks for it. The same text is also in the .txt file that comes with this report.

IC3 COMPLAINT TEXT · COPY AND PASTE

===== IC3 COMPLAINT TEXT: COPY AND PASTE INTO THE IC3 FORM =====

SAMPLE: EXAMPLE DATA ONLY. These are made-up addresses and transaction IDs. Do not file this text.

PART 1. DESCRIPTION OF WHAT HAPPENED (paste into the incident description box)

I am reporting a cryptocurrency fraud on the Solana blockchain. On March 3, 2026 a person I met in a Telegram trading group (username @example_vault_admin) persuaded me to send 42 SOL, about \$6,300, to a "staking vault" that promised 3% a day. The vault was an ordinary wallet and I could not withdraw. I lost about \$6,300.

My payments to the scammer (times are ET):

1. Mar 3, 2026 9:12 PM ET: I sent 42.0 SOL (about \$6,300) from my wallet
EXAMPLEMeJ2VCj8YzsaqaqccwNecXZScd6CnCBHMzVqd to EXAMPLEVau9nw1Mct1c6sQMRZNYzRrBGLMPStMULQ59r.
Transaction ID:
EXAMPLETXFAAecDViQK2e43qqmfcoV2KpVSt2qA4RhBPxXfDXa7rPwaQTwdUQXYgxXXf9ZPabVa1VZKi62draYP

Where the money went next, from public blockchain records (each step can be checked by its transaction ID):

Step 2: Mar 3, 2026 9:20 PM ET: 41.9 SOL from EXAMPLEVau9nw1Mct1c6sQMRZNYzRrBGLMPStMULQ59r to
EXAMPLESdCvdzPTR3KhKLBURk6AmT1KYrYsP96r8R. Transaction ID:
EXAMPLETXKPPQtVaRdRoXQwz89ysDLZ88ZsUUNDWH5WdbebWpmUSrSfXJvzUCUF8xNGfqcWicFsFvqTnjqnqLyCS
(appears to be: Intermediate)

Step 3: Mar 3, 2026 9:31 PM ET: 41.9 SOL to 6,061 USDC from
EXAMPLESdCvdzPTR3KhKLBURk6AmT1KYrYsP96r8R to EXAMPLECN6iYwA4DgYA4R5xc5yCVmSZ58FqvXgKtZbz2.
Transaction ID:
EXAMPLETXSokGUQzbMUPgx5WKzdRRW6FXhkZ4W3uR2UWnPaGjs2EcRvhyU7Ua7BGtuuTkNw5hCcUoMV8LXEYasJ
(appears to be: Swap)

Step 4: Mar 3, 2026 9:52 PM ET: 6,050 USDC from EXAMPLECN6iYwA4DgYA4R5xc5yCVmSZ58FqvXgKtZbz2 to
EXAMPLEExy1h7E71dz8ZVWLFZPYQsS2VmXQTeLj81bYm. Transaction ID:
EXAMPLETXvXhbhi3va4euXPTFebkshv4qmEz8onQxwS79tSMMPogFKKBjrgJ7ct56T6DEEUuRTizQcBpUmj6v2zA
(appears to be: Exchange deposit (labeled))

The money appears to have reached these exchange deposit addresses:
 EXAMPLEExy1h7E71dz8ZVWLFZPYQsS2VmXQTeLj81bYm (EXAMPLE large exchange, deposit address). I ask that the exchange be contacted to identify the account holder.

I have kept the original records (wallet history, screenshots and messages) and can provide them if an investigator asks.

PART 2. TRANSACTION IDs (one per line; paste each into a transaction ID / hash field)

1. Mar 3, 2026 9:12 PM ET (my payment):
 EXAMPLETXFAAecDViQK2e43qqmfcoV2KpVSt2qA4RhbpXxFdDXa7rPwaQTWdUQXYgxXXf9ZPabVa1VZKi62draYP
2. Mar 3, 2026 9:20 PM ET (step 2):
 EXAMPLETXKPPQtVaRdRoXQwz89ysDLZ88ZsUUUNDWH5WdbebWpmUSrSfXJvzUCUF8xNGfqcWicFsFvqTnqnqoLYCS
3. Mar 3, 2026 9:31 PM ET (step 3):
 EXAMPLETXTSokGUQzbMUPgx5WKzdRRW6FXhkZ4W3uR2UwnPaGjs2EcRvhyU7Ua7BGtuuTKnW5hCcUoMV8LXEYasJ
4. Mar 3, 2026 9:52 PM ET (step 4):
 EXAMPLETXvXhbhi3va4euXPTFebkshv4qmEz8onQxwS79tSMMPogFKKBjrgJ7ct56T6DEEUuRTizQcBpUmj6v2ZA

PART 3. ADDRESSES (paste into the cryptocurrency address fields)

My wallet address(es):

EXAMPLEMeJ2VCj8YzsaaaqccwNeCXZScd6CnCBHMzVqd

Addresses I sent money to:

EXAMPLEVau9nw1MCt1c6sQMRZNYzRrBGLMPStMULQ59r

Addresses the money moved to next:

EXAMPLEsdCvdozPTR3KhKLBLUrkw6AmT1KYrYsP96r8R

EXAMPLECN6iYwA4DgYA4R5xc5yCVmSZ58FqvXgKtZbz2

Likely exchange deposit addresses:

EXAMPLEExy1h7E71dz8ZVWLFZPYQsS2VmXQTeLj81bYm (EXAMPLE large exchange, deposit address)

===== END OF IC3 COMPLAINT TEXT =====

How to file, in order

1. FBI IC3 (type www.ic3.gov yourself): Paste the text into the IC3 form and keep this PDF in case an investigator asks for it. Paste the description, then each transaction ID and address. Filing is free.
2. FTC (reportfraud.ftc.gov).
3. Your state attorney general (in Michigan: 877-765-8388 or michigan.gov/ag/complaints) and your local police. Exchanges often ask for a police report before they act.
4. If you sent a bank wire or transfer in the last few days, call your bank first.
5. Keep a copy of everything. IC3 never asks for money and has no social media; anyone offering to recover your funds for a fee is a scammer.

Step-by-step help: walletties.com/ic3-guide (free).

Want the complete picture? The \$99 Full Investigation adds up to 6 hours of automated tracing with no wallet cap, a wallet map, Token Ties (coins the same wallets appear to be tied to) and a list of open leads, delivered within 3 days. We'll never suggest a report that costs more than makes sense for what you lost.

WalletTies is not a recovery service, law firm, or law enforcement, and is not affiliated with the FBI. This report is informational, based on public blockchain data, for you to file yourself.