Your IC3 Complaint

Submission ID:	93045798a9294c7aa20a1bbeb3d71afc
Date Filed:	3/7/2025 8:35:20 PM EST
Were you the one affected in this incident?	Yes

Your Contact Information

Name:	Chandra Kishore Danduri
Phone Number:	4088170099
Email Address:	chandra.kishore180994@gmail.com

Complainant Information

Name:	Chandra Kishore Danduri
Address:	751 Pomeroy Ave
City:	Santa Clara
Country:	United States of America
State:	California
Zip Code/Route:	95051
Phone Number:	4088170099
Email Address:	chandra.kishore180994@gmail.com

Business Information

Is this on behalf of a business that was targeted by a Cyber incident?	No

Financial Transaction(s)

Did you send or lose money in the incident?	Yes
What was your total loss amount?	2,874.00

Transaction Type:	Cryptocurrency/Crypto ATM
Was the money sent or lost?	Yes
Transaction Amount:	1,362.00
Transaction Date:	03/07/2025
Did you contact your bank, financial institution, or cryptocurrency exchange?	No
Type of Cryptocurrency:	USDC
Transaction ID/Hash:	0xed20e78caa70c45910196a57b2b971be0527b6860c9f179f44136547f0
Originating Wallet Address:	0xF2a5eA08aB57356E601513AD7087fDAe8dbe7c76
Recipient Wallet Address:	0x99dB0581972c82c6bfAeAbbF5371B71C321A9538

Transaction Type:	Cryptocurrency/Crypto ATM
Was the money sent or lost?	Yes
Transaction Amount:	1,512.00
Transaction Date:	03/07/2025
Did you contact your bank, financial institution, or cryptocurrency exchange?	No
Type of Cryptocurrency:	STAR10
Transaction ID/Hash:	0x57cb8a335bbf2e70c7da19507f1dfe03220bef1370ff77fde6049402b6c3
Originating Wallet Address:	0xF2a5eA08aB57356E601513AD7087fDAe8dbe7c76
Recipient Wallet Address:	0x99dB0581972c82c6bfAeAbbF5371B71C321A9538

Information About The Subject(s)

Name:	Unknown

Description of Incident

Provide a description of the incident and how you (or those you are filling this out on behalf of) were victimized. Provide information not captured elsewhere in this complaint form:

On March 7, 2025, my Trust Wallet was compromised, leading to unauthorized transactions where my cryptocurrency assets were stolen and transferred without my consent.

Initially, 53,918.66 STAR10 tokens (approximately $1,524.84 USD) were transferred from my wallet. The attacker then swapped these tokens into Binance-Pegged USDC using PancakeSwap SwapRouter V3 and subsequently transferred the converted funds to another wallet.

Shortly after, a second unauthorized transaction took place, where an additional $1,362.66 USDC was stolen and transferred through multiple wallet addresses in an attempt to launder the funds.

I have identified the following transaction details related to the theft:

Transaction Details (First Theft - STAR10 Tokens → USDC)
My Wallet Address (Originating):
[0xF2a5eA08aB57356E601513AD7087fDAe8dbe7c76]
Hacker's Wallet Address (Recipient):
[0x99dB0581972c82c6bfAeAbbF5371B71C321A9538]
Transaction Hash (Stolen Funds Transfer):
[0x57cb8a335bbf2e70c7da19507f1dfe03220bef1370ff77fde6049402b6c3e909]
Transaction Hash (Swap to USDC):
[0x90a971ec3f1be4c0d3461c32957ef15bc51c52d9f119ec8beeb1bdb56c1b3c2d]

Transaction Details (Second Theft - USDC)
My Wallet Address (Originating):
[0xF2a5eA08aB57356E601513AD7087fDAe8dbe7c76]
Hacker's Wallet Address (Recipient):
[0x99dB0581972c82c6bfAeAbbF5371B71C321A9538]
Transaction Hash (Stolen Funds Transfer):
[0xed20e78caa70c45910196a57b2b971be0527b6860c9f179f44136547f0268d89]
Transaction Hash (Wallet Hoping / Money Laundering):
[0x3b81405241c5018cb8336c0646f87ecf22a551adba6af6de897fc32bd6dc16cb]

Other Information

If an email was used in this incident, please provide a copy of the entire email including full email headers.

This incident involved the unauthorized transfer of cryptocurrency assets from my Trust Wallet. The attacker used multiple wallet addresses and PancakeSwap SwapRouter V3 to swap my tokens into Binance-Pegged USDC and attempted to launder the funds by transferring them through various intermediary wallets.

1. Transaction Metadata
First Theft (STAR10 to USDC)

My Wallet Address: 0xF2a5eA08aB57356E601513AD7087fDAe8dbe7c76
Hacker's Wallet Address: 0x99dB0581972c82c6bfAeAbbF5371B71C321A9538
Transaction Hash (Stolen Funds Transfer):
0x57cb8a335bbf2e70c7da19507f1dfe03220bef1370ff77fde6049402b6c3e909
Transaction Hash (Swap to USDC):
0x90a971ec3f1be4c0d3461c32957ef15bc51c52d9f119ec8beeb1bdb56c1b3c2d
Second Theft (USDC)

My Wallet Address: 0xF2a5eA08aB57356E601513AD7087fDAe8dbe7c76
Hacker's Wallet Address: 0x99dB0581972c82c6bfAeAbbF5371B71C321A9538
Transaction Hash (Stolen Funds Transfer):
0xed20e78caa70c45910196a57b2b971be0527b6860c9f179f44136547f0268d89
Transaction Hash (Wallet Hopping / Money Laundering):
0x3b81405241c5018cb8336c0646f87ecf22a551adba6af6de897fc32bd6dc16cb

The attacker first swapped STAR10 tokens into USDC via PancakeSwap SwapRouter V3.
The stolen USDC was transferred through multiple wallets in quick succession.
Some transactions indicate a possible deposit into an exchange, where the funds might still be recoverable.

Are there any other witnesses or persons affected by this incident?

Yes, My RoomMate is the witness.

If you have reported this incident to other law enforcement or government agencies, please provide the name, phone number, email, date reported, report number, etc.

Urgent intervention is required to stop further movement of funds.

- Freeze the hacker's wallet if possible.
- Check if the final wallet is linked to a centralized exchange (CEX) and request a transaction block.

- Blacklist the hacker's wallet to prevent future scams.
- Assist in tracking and recovering my stolen assets.

Is this an update to a previously filed complaint? No

Privacy & Signature:

The collection of information on this form is authorized by one or more of the following statutes: 18 U.S.C. § 1028 (false documents and identity theft); 1028A (aggravated identity theft); 18 U.S.C. § 1029 (credit card fraud); 18 U.S.C. § 1030 (computer fraud); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C 2318B (counterfeit and illicit labels); 18 U.S.C. § 2319 (violation of intellectual property rights); 28 U.S.C. § 533 (FBI authorized to investigate violations of federal law for which it has primary investigative jurisdiction); and 28 U.S.C. § 534 (FBI authorized to collect and maintain identification, criminal information, crime, and other records).

The collection of this information is relevant and necessary to document and investigate complaints of Internet-related crime. Submission of the information requested is voluntary; however, your failure to supply requested information may impede or preclude the investigation of your complaint by law enforcement agencies.

The information collected is maintained in one or more of the following Privacy Act Systems of Records: the FBI Central Records System, Justice/FBI-002, notice of which was published in the Federal Register at 63 Fed. Reg. 8671 (Feb. 20, 1998); the FBI Data Warehouse System, DOJ/FBI-022, notice of which was published in the Federal Register at 77 Fed. Reg. 40631 (July 10, 2012). Descriptions of these systems may also be found at www.justice.gov/opcl/doj-systems-records#FBI. The information collected may be disclosed in accordance with the routine uses referenced in those notices or as otherwise permitted by law. For example, in accordance with those routine uses, in certain circumstances, the FBI may disclose information from your complaint to appropriate criminal, civil, or regulatory law enforcement authorities (whether federal, state, local, territorial, tribal, foreign, or international). Information also may be disclosed as a routine use to an organization or individual in both the public or private sector if deemed necessary to elicit information or cooperation from the recipient for use by the FBI in the performance of an authorized activity. "An example would be where the activities of an individual are disclosed to a member of the public in order to elicit his/her assistance in [FBI's] apprehension or detection efforts." 63 Fed. Reg. 8671, 8682 (February 20, 1998).

By typing my name below, I understand and agree that this form of electronic signature has the same legal force and effect as a manual signature. I affirm that the information I provided is true and accurate to the best of my knowledge. I

understand that providing false information could make me subject to fine, imprisonment, or both. (Title 18, U.S.Code, Section 1001)

Digital Signature: Chandra Kishore Danduri