SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

RADHIKA ADVANI, on behalf of herself and individuals similarly situated	)	Index No. 156048-2026
Plaintiff,	)	
-against-	)	
JOHN DOE NOS. 1-25	)	
Defendants.	)	

DECLARATION OF MAYA VICK

I, Maya Vick, declare under penalty of perjury under the laws of the State of New York that the foregoing is true and correct. I affirm this 19th day of May, 2026 under the penalties of perjury under the laws of New York, which may include a fine or imprisonment, that the foregoing is true, except as to matters alleged on information and belief and as to those matters I believe it to be true, and I understand that this document may be filed in an action or proceeding in a court of law.

I. INTRODUCTION

1. I am over eighteen years of age, of sound mind, and competent to make this declaration. The statements contained herein are based on my personal knowledge, my professional training and experience, and information derived from forensic blockchain analysis conducted by Inca Digital using investigative methodologies and data sources commonly relied upon by experts in the field of cryptocurrency investigations.

2. I am employed by Inca Digital, a digital asset intelligence company that provides data analytics, blockchain forensic analysis, and investigative support to cryptocurrency

exchanges, financial institutions, regulators, and government agencies. Inca Digital conducts investigations into digital asset markets and cryptocurrency-related criminal activity, including fraud, market manipulation, and illicit financial flows. Additional information about Inca Digital and its work is available at https://inca.digital.

3. In my role at Inca Digital, I have conducted numerous investigations involving cryptocurrency fraud schemes, including schemes commonly referred to as "pig-butchering." These investigations typically involve tracing cryptocurrency transactions across blockchain networks in order to identify wallet infrastructure, intermediary routing wallets, and custodial exchange deposit addresses associated with fraudulent activity.

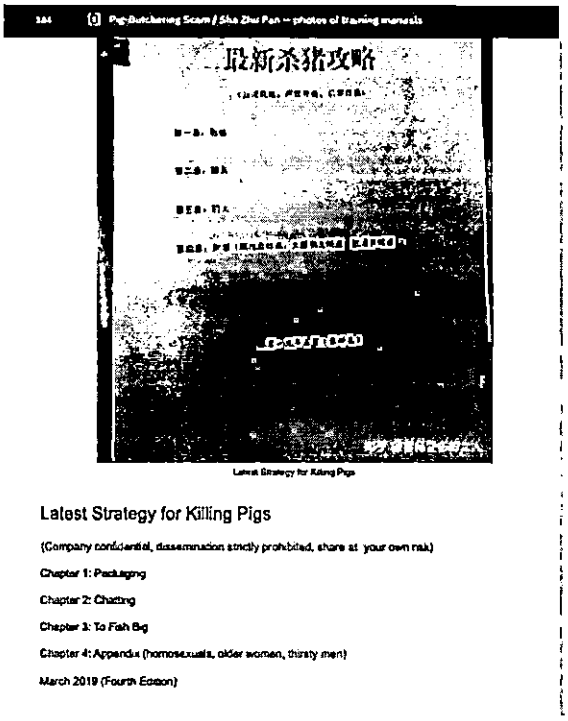
4. In connection with this matter, I have reviewed Plaintiff Radhika Advani's Verified Complaint and supporting materials and am familiar with the facts alleged therein. I have also reviewed blockchain transaction data and conducted forensic blockchain analysis relating to cryptocurrency transfers made by Plaintiff.

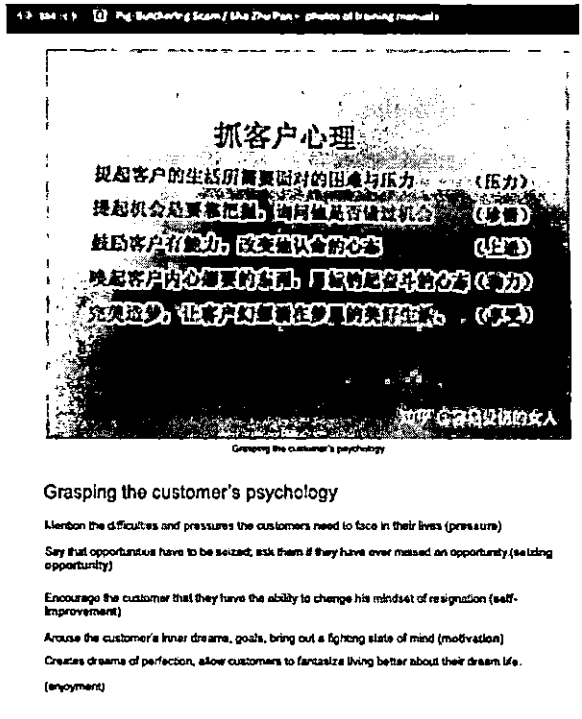
5. Based on my education, training, and experience investigating cryptocurrency fraud schemes, the conduct described in the Verified Complaint is consistent with a type of transnational cryptocurrency investment fraud commonly referred to as a "pig-butchering"[1] scheme, sometimes referred to by the Chinese term *Sha Zhu Pan*. In such schemes, perpetrators typically establish fictitious online identities and communicate with victims through messaging

[1] ProPublica recently published an in-depth investigation of pig butchering, describing how criminal syndicates operate, often by forcing human trafficking victims to perpetrate the schemes against their will, including the following process: "1) Create a fake identity. 2) Initiate contact. 3) Win the trust of the target. 4) Sign them up. 5) Get them to put real money into the fake account. 6) "Prove" that it's legitimate. 7) Manipulate them into investing more. 8) Cut them off. 9) Use their desperation to your advantage. 10) Taunt and depart." See Cezary Podkul, *What's a Pig Butchering Scam? Here's How to Avoid Falling Victim to One.* PROPUBLICA, Sept. 19, 2022, https://www.propublica.org/article/whats-a-pig-butchering-scam-heres-how-to-avoid-falling-victim-to-one. As described below, Defendants likewise followed these steps.

platforms or social media in order to gain trust and induce victims to transfer cryptocurrency to fraudulent investment platforms controlled by the perpetrators.

6. Based on my experience investigating these schemes, many pig-butchering operations are conducted by organized transnational groups operating in East and Southeast Asia. Among other evidence, Inca Digital has obtained an operations manual of one such transnational criminal group as displayed below. The manual provides guidance in setting up and operating a pig butchering scheme.





Screenshots from Pig Butchering Operations Manual

7. Fraudulent cryptocurrency trading platforms used in pig-butchering schemes frequently attempt to mimic legitimate businesses and exchanges in order to create the appearance of credibility. Based on my experience investigating similar schemes, such platforms often use domain names, branding, or other design elements that resemble established businesses or cryptocurrency exchanges. The websites referenced in the Verified Complaint, wendywutours-

tours.com and wendywutours-adventure.com, appear consistent with this pattern in that it closely resembles the name of the legitimate travel and tourism business known as https://www.wendywutours.com and was presented to Plaintiff as a legitimate business associated with the travel and tourism industry.

8. Platforms used in these schemes commonly display fabricated account balances and fictitious profits to encourage victims to transfer additional cryptocurrency. Victims may initially be permitted to withdraw small amounts of cryptocurrency in order to increase their confidence in the platform before larger deposits are requested. Once victims have transferred substantial amounts of cryptocurrency, the perpetrators often impose fabricated withdrawal conditions—such as purported taxes, margin payments, credit imbalances or other fees, in order to extract additional funds while preventing any meaningful withdrawal of assets.

9. Based on my experience investigating cryptocurrency exchanges and digital asset platforms, legitimate exchanges do not require customers to pay capital gains taxes, margin payments, or other deposits as a condition of withdrawing funds from their accounts. Such representations are commonly used in fraudulent cryptocurrency investment schemes.

10. I conducted blockchain forensic analysis to trace cryptocurrency transfers associated with Plaintiff's transactions. The purpose of this analysis is to identify the blockchain wallet addresses that received Plaintiff's cryptocurrency, trace the subsequent movement of those assets across intermediary wallets, and determine whether those assets were ultimately deposited into custodial cryptocurrency exchanges where they may remain subject to restraint. This analysis was conducted using blockchain forensic tools and methodologies commonly used in digital asset investigations, including transaction graph analysis, wallet clustering techniques, and exchange attribution databases.

The results of my blockchain tracing analysis are described below.

II. TRACING THE MOVEMENT OF RADHIKA ADVANI'S STOLEN FUNDS

A. Radhika Advani's Initial Transactions

11. Plaintiff, Radhika Advani, (hereinafter referred to as the "Victim"), was contacted on Facebook by a purported representative of "Wendy Wu Tours" for a "task gig," in which the Victim was offered money to complete an assorted array of tasks. The victim was lulled into a false sense of security due to being connected to a Telegram group where other participants confirmed that these tasks were legitimate – the Victim now believes that these may have been fraudulent or otherwise paid participants. These tasks eventually began to require funds in order to proceed with accepting higher value tasks, ultimately resulting in the Victim transferring approximately **$168,000** in cryptocurrency.

12. Blockchain tracing has verified that between October 3 and November 27, 2024, the Victim transferred a total of **$163,618.94** in cryptocurrency across 11 cryptocurrency transactions to Intake Wallets—the first known scam-controlled addresses to which perpetrators directed the Victim to send assets.

13. From those wallets, the perpetrators systematically moved funds through a series of additional transactions—sending the funds through a maze of other addresses until they ultimately reached Exchange-Hosted Deposit Wallets.

14. The table below details all transactions where the Victim transferred funds to Intake Wallet addresses provided by the perpetrators, which are listed in the "To Address" column.

Transfer	Date/Time	From Exchange	From Address	To Address	Asset Type	Asset Amount	USD Equivalent
1	10/3/2024 20:41:11 UTC	Coinbase	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x45ac2da729eda225b82f4835dec0e35a1dc13233	USDC	2,943.56	$2,943.56

2	10/04/2024 16:39:11 UTC	Coinbase	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0xb5e68aebdf6df4acae7717cd6dd51c1a1ae23a80	USDC	5,413.38	$5,413.38
3	11/15/2024 00:29:11 UTC	Coinbase	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x104c1c1281ff75f6b183d53450ef0925c46a62bb	USDC	7,947.00	$7,947.00
4	11/15/2024 0:29:11 UTC	Coinbase	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0xbf18552042549e0cdba5e5a95378e76ac1cc4c6e	USDC	17,000.00	$17,000.00
5	11/22/2024 17:52:11 UTC	Coinbase	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0xD125742e32486F681BF2D32a339cd7a6bEC77c51	USDC	10,000.00	$10,000.00
6	11/22/2024 18:08:11 UTC	Coinbase	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0xeFC45259FB434F1538f5faC90A5809be352c29b3	USDC	10,000.00	$10,000.00
7	11/22/2024 18:16:11 UTC	Coinbase	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0xeFC45259FB434F1538f5faC90A5809be352c29b3	USDC	10,000.00	$10,000.00
8	11/22/2024 18:26:59 UTC	Coinbase	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0xeFC45259FB434F1538f5faC90A5809be352c29b3	USDC	9,980.00	$9,980.00
9	11/26/2024 20:45:11 UTC	Coinbase	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x7AD55815e9397d9615A4886E4b87a6479102B8fF	USDC	10,000.00	$10,000.00
10	11/26/2024 20:56:11 UTC	Coinbase	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x7AD55815e9397d9615A4886E4b87a6479102B8fF	USDC	17,800.00	$17,800.00
11	11/27/2024 16:13:11 UTC	Coinbase	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x44619c45ab4bd180d4cfd4d8565b397d000ca7df	USDC	62,535.00	$62,535.00

15. In total, Ms. Advani sent funds to 8 different Intake Wallets:

- **Intake Wallet #1:** 0x45ac2da729eda225b82f4835dec0e35a1dc13233
- **Intake Wallet #2:** 0xb5e68aebdf6df4acae7717cd6dd51c1a1ae23a80
- **Intake Wallet #3:** 0x104c1c1281ff75f6b183d53450ef0925c46a62bb
- **Intake Wallet #4:** 0xbf18552042549e0cdba5e5a95378e76ac1cc4c6e
- **Intake Wallet #5:** 0xD125742e32486F681BF2D32a339cd7a6bEC77c51
- **Intake Wallet #6:** 0xeFC45259FB434F1538f5faC90A5809be352c29b3
- **Intake Wallet #7:** 0x7AD55815e9397d9615A4886E4b87a6479102B8fF
- **Intake Wallet #8:** 0x44619c45ab4bd180d4cfd4d8565b397d000ca7df

16. Funds from the Intake Wallet were ultimately transferred to Exchange-Hosted Deposit Wallets, hosted at Binance, BitGet, Crypto.com, HTX, Kraken, MaskEx, Newton Canada, OKX, Revolut, and Wealthsimple.

B. Flow of Funds Analysis.

Overview

17. Forensic blockchain analysis confirms that the Victim's funds were systematically routed through transaction pathways designed to obscure their origin.

18. Funds were routed through intermediary wallets, including Pivot Wallets, where they were combined, split, and transferred across multiple additional addresses. These structured movements demonstrate an intent to break direct transaction links, disrupt traceability, and hinder asset recovery. The assets were ultimately deposited into the Exchange-Hosted Deposit Wallets, the addresses of which are listed in section "V. Wallets to Freeze" herein.

Role of Pivot Wallets in Fund Movement

19. Bad actors use Pivot Wallets as central points in the laundering process to consolidate stolen funds from multiple victims. By aggregating and redistributing assets, these wallets obscure direct transactional links, making it harder to trace funds from their original sources to final destinations. Forensic blockchain analysis conducted in this case successfully traced the movement of funds through these wallets, revealing a coordinated scheme.

Specifically identified Pivot Wallet addresses in this case include:

- **Pivot Wallet #1: 0x8a80396a4b63b3efe1b7995e8118d313f9f6f9ba**
- **Pivot Wallet #2: 0x3e3bc76bf2db5c27e56cc5afa8e55e97ecd10e5c**
- **Pivot Wallet #3: 0x7462833731df0868abad34a1572b1930012427c5**

Traced Pathways of Victim Funds

20. Pathways describe how funds move from Victim Wallets to Exchange Deposit Wallets. The analysis in this case identified two pathway types, categorized as Pathway 1 and Pathway 2.

21. These pathways both show different levels of complexity. Pathway 1 involved the transfer of victim funds into Intake Wallets, which then deposit funds directly into Pivot Wallets which then transfer through various Intermediary Wallets before ultimately reaching Exchange-Hosted Deposit Wallets. Pathway 2 is similar but involves the usage of Intermediary Wallets before reaching the Pivot Wallets.

22. Below is an analysis of Pathway 1.

Pathway 1: Transfer to Intake Wallet to Pivot Wallet to Additional Intermediary Wallets to Exchange-Hosted Deposit Wallets

Transfers 3-11

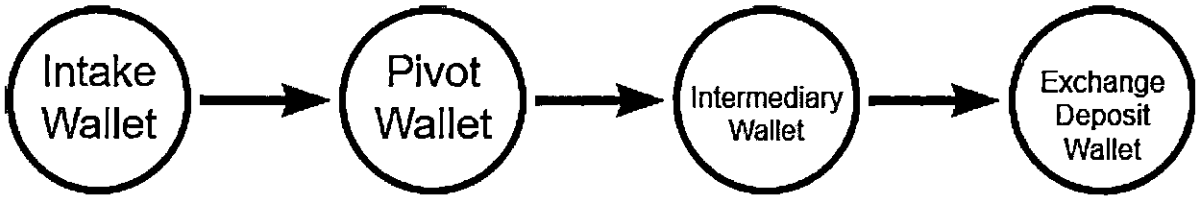
• The Victim transferred funds from their personally controlled wallet to different Intake Wallets:

Intake Wallet #3: 0x104c1c1281ff75f6b183d53450ef0925c46a62bb
Intake Wallet #4: 0xbf18552042549e0cdba5e5a95378e76ac1cc4c6e
Intake Wallet #5: 0xD125742e32486F681BF2D32a339cd7a6bEC77c51
Intake Wallet #6: 0xeFC45259FB434F1538f5faC90A5809be352c29b3
Intake Wallet #7: 0x7AD55815e9397d9615A4886E4b87a6479102B8fF
Intake Wallet #8: 0x44619c45ab4bd180d4cfd4d8565b397d000ca7df

• Funds were then aggregated at **Pivot Wallet #1: 0x8a80396a4b63b3efe1b7995e8118d313f9f6f9ba** and **#2: 0x3e3bc76bf2db5c27e56cc5afa8e55e97ecd10e5c** before being routed through multiple different intermediary wallets.

• After layering transactions across multiple wallets, the funds were ultimately deposited into Deposit Wallets at MaskEX, Binance, and OKX

• This movement is illustrated in the Simplified Flow of Funds Graph below.



23. Below is an analysis of Pathway 2.

Pathway 2: Transfer to Intake Wallet to Intermediary Wallets to Pivot Wallet to Additional Intermediary Wallets to Exchange-Hosted Deposit Wallets

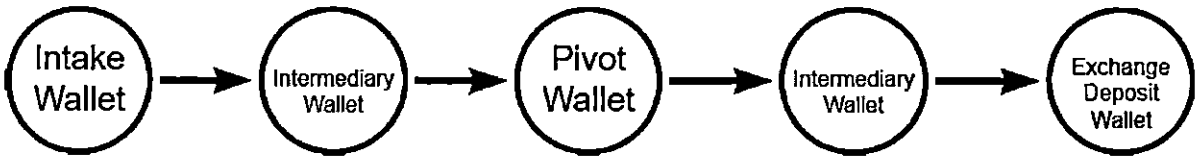
Transfers 1, 2

• The Victim transferred funds from their personally controlled wallet to Intake Wallets 0x45ac2da729eda225b82f4835dec0e35a1dc13233 and 0xb5e68aebdf6df4acae7717cd6dd51c1a1ae23a80.

• Funds first passed through an intermediary wallet and were then aggregated at **Pivot Wallet #3: 0x7462833731df0868abad34a1572b1930012427c5** and then passed through through 15 additional intermediary wallets.

• After layering transactions across multiple wallets, the funds were ultimately deposited into Deposit Wallets at Newton Canada, Kraken, and Crypto.com.

• This movement is illustrated in the Simplified Flow of Funds Graph below.



C. Individual Transfer Details and Tracing Graphs

Transfer 1

24. The Victim transferred funds from their personally controlled wallet to Intake Wallet 0x45ac2da729eda225b82f4835dec0e35a1dc13233.

25. Funds first passed through one intermediary wallet before being aggregated at Pivot Wallet 0x7462833731df0868abad34a1572b1930012427c5 and then passed through one intermediary wallet before distribution to Exchange-Hosted Deposit Wallets at Metamask, Newton Canada, and Kraken.

Transfer 2

26. The Victim transferred funds from their personally controlled wallet to Intake Wallet 0xb5e68aebdf6df4acae7717cd6dd51c1a1ae23a80.

27. Funds first passed through one intermediary wallet before being aggregated at Pivot Wallet 0x7462833731df0868abad34a1572b1930012427c5 and then passed through one intermediary wallet before distribution to Exchange-Hosted Deposit Wallets at Metamask, Newton Canada, and Kraken.

Transfer 3

28. The Victim transferred funds from their personally controlled wallet to Intake Wallet 0x104c1c1281ff75f6b183d53450ef0925c46a62bb.

29. Funds were deposited and aggregated at Pivot Wallet 0x8a80396a4b63b3efe1b7995e8118d313f9f6f9ba and then passed through intermediary wallets before distribution to Exchange-Hosted Deposit Wallets at MaskEX, Binance, and OKX.

Transfer 4

30. The Victim transferred funds from their personally controlled wallet to Intake Wallet 0xd125742e32486f681bf2d32a339cd7a6bec77c51.

31. Funds were deposited and aggregated at Pivot Wallet 0x8a80396a4b63b3efe1b7995e8118d313f9f6f9ba and then passed through intermediary wallets before distribution to Exchange-Hosted Deposit Wallets at MaskEX, Binance, and OKX.

Transfer 5

32. The Victim transferred funds from their personally controlled wallet to Intake Wallet 0xbf18552042549e0cdba5e5a95378e76ac1cc4c6e.

33. Funds were deposited and aggregated at Pivot Wallet 0x3e3bc76bf2db5c27e56cc5afa8e55e97ecd10e5c and then passed through four intermediary wallets before distribution to Exchange-Hosted Deposit Wallets at Binance, Bitget, Crypto.com, and Wealthsimple.

Transfers 6-8

34. The Victim transferred funds from their personally controlled wallet to Intake Wallet 0xefc45259fb434f1538f5fac90a5809be352c29b3.

35. Funds were deposited and aggregated at Pivot Wallet 0x8a80396a4b63b3efe1b7995e8118d313f9f6f9ba and then passed through intermediary wallets before distribution to Exchange-Hosted Deposit Wallets at MaskEX, Binance, and OKX.

Transfers 9-10

36. The Victim transferred funds from their personally controlled wallet to Intake Wallet 0x7ad55815e9397d9615a4886e4b87a6479102b8ff.

37. Funds were deposited and aggregated at Pivot Wallet 0x3e3bc76bf2db5c27e56cc5afa8e55e97ecd10e5c and then passed through four intermediary wallets before distribution to Exchange-Hosted Deposit Wallets at Binance, Bitget, Crypto.com, and Wealthsimple.

Transfer 11

38. The Victim transferred funds from their personally controlled wallet to Intake Wallet 0x44619c45ab4bd180d4cfd4d8565b397d000ca7df.

39. A portion of the funds were deposited and aggregated at Pivot Wallet 0x3e3bc76bf2db5c27e56cc5afa8e55e97ecd10e5c and then passed through four intermediary wallets before distribution to Exchange-Hosted Deposit Wallets at Binance, Bitget, Crypto.com, and Wealthsimple.

40. Another portion of funds out of this Intake Wallet were deposited and aggregated at Pivot Wallet 0x8a80396a4b63b3efe1b7995e8118d313f9f6f9ba and then passed through intermediary wallets before distribution to Exchange-Hosted Deposit Wallets at MaskEX, Binance, and OKX.

III. BROADER FRAUD NETWORK AND CLASS IMPACT

A. Identifying the Broader Fraud Network

41. Forensic blockchain analysis confirms that the theft of the Victim's assets was not an isolated incident but part of a systematic fraud scheme, structured to obscure transaction origins and facilitate large-scale misappropriation of cryptocurrency. The same Pivot Wallets that received the Victim's funds also show structured inflows from multiple unrelated wallets following similar transaction patterns, confirming their role as collection points in a broader fraud network.

How Pivot Wallets Reveal Coordinated Theft Scheme

42. Pivot Wallets are essential to identifying the affected group or class of victims because they establish that multiple victims' funds were controlled by the same bad actor or group. These wallets function as aggregation points where stolen funds from numerous victims converge, demonstrating a systematic, coordinated scheme. Unlike isolated incidents of theft, where funds may follow unique or random paths, the presence of Pivot Wallets reveals a pattern of consolidation and redistribution of misappropriated assets. By consolidating funds from unrelated

victims into a single location, Pivot Wallets establish a centralized point of control, linking disparate victims to a unified fraudulent operation.

B. Estimated Class Impact

43. By tracing inflows into known Pivot Wallets, forensic analysts identified several additional victim wallets that followed the same structured fund movement patterns as the Victim's transactions. These wallets exhibited identical laundering behaviors, confirming that they belong to additional victims of the same fraud scheme:

- **Matching structured transaction pathways** observed across multiple cases, following the same laundering techniques.
- **Pivot Wallet aggregation**, confirming that multiple victims' funds were pooled in the same intermediary wallets before onward movement.
- **Consistent transaction behaviors** across victims, reinforcing the presence of a coordinated fraud operation.

44. **Estimated Total Class-Wide Losses:** Class-wide losses are estimated to be approximately **$31,077,915 USD**, based on cumulative victim deposits into identified Pivot Wallets.

45. The funds were distributed across the exchanges listed below:

- Binance
- BitGet
- Crypto.com
- HTX
- Kraken
- MaskEx
- Newton Canada
- OKX
- Revolut

- Wealthsimple

46. The Estimated Total Class-Wide Losses represents the total financial impact on victims. The Estimated Total Funds Traced to Exchange Deposit wallets reflects the portion of those total losses likely traceable to identifiable exchange accounts. The difference between the estimated class losses and the amount traced to Deposit Wallets reflects a combination of currently unrecoverable funds—held in a non-exchange wallet—and untraceable funds that have been sufficiently laundered in ways that break the chain of traceable transactions.

47. While both figures are relevant to understand the extent and movement of stolen assets, differentiating helps clarify the full scope of victim losses versus the amount that may be subject to a freeze and, ultimately, recovery.

IV. OBSERVED LAUNDERING AND FRAUD INDICATORS

48. Forensic analysis confirms behavioral and technical patterns consistent with fraudulent activity, including structured fund movements that align with known laundering methodologies and existing fraud indicators implicating perpetrators' infrastructure, including the following:

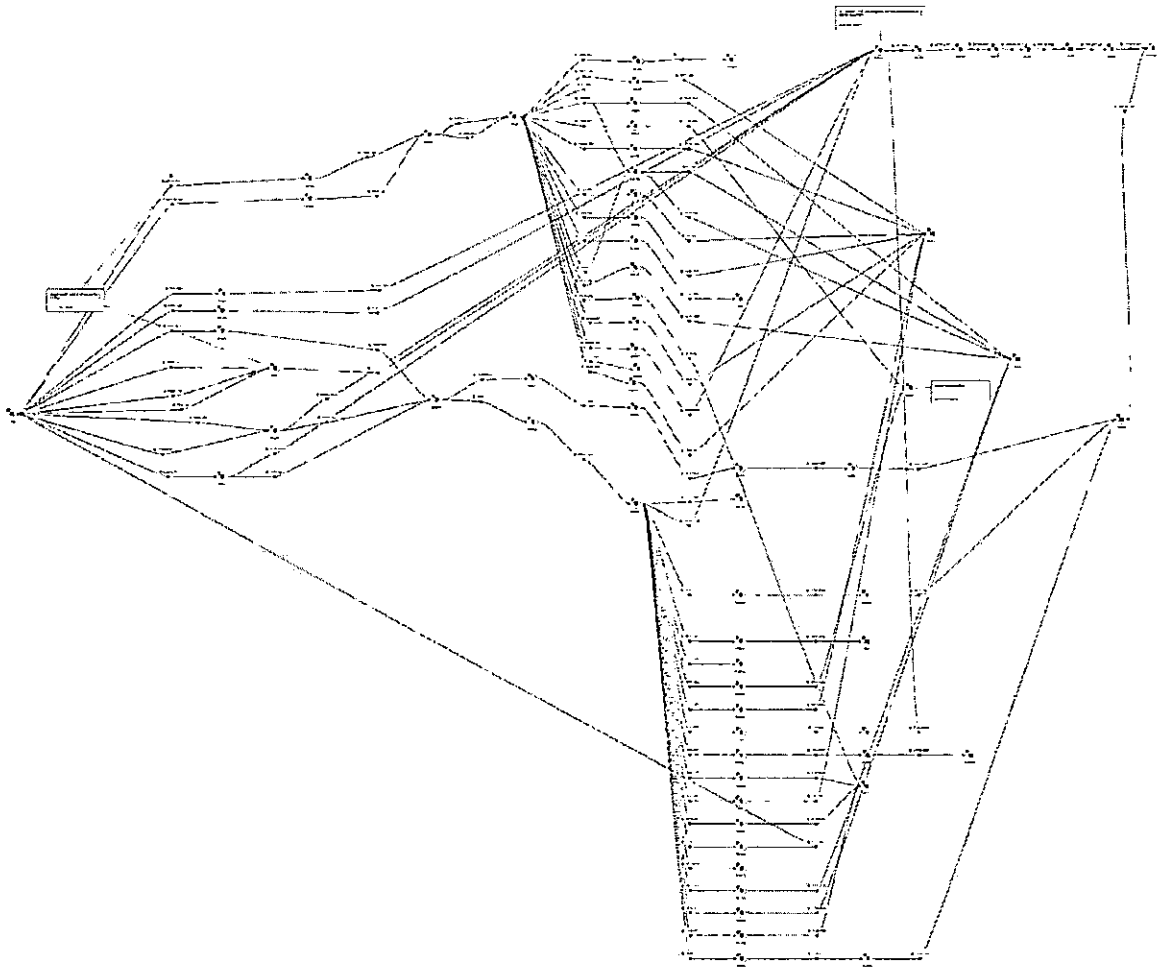
- **Token conversions on Tokenlon** to obscure fund origins (e.g., swapping ETH for privacy tokens like Monero or Dash to break traceability).
- **Partial splits into smaller amounts** to evade anti-money laundering detection thresholds (*e.g.,* splitting $500,000 into multiple transactions under $10,000 to bypass exchange reporting requirements).

A. Identified Laundering Techniques:

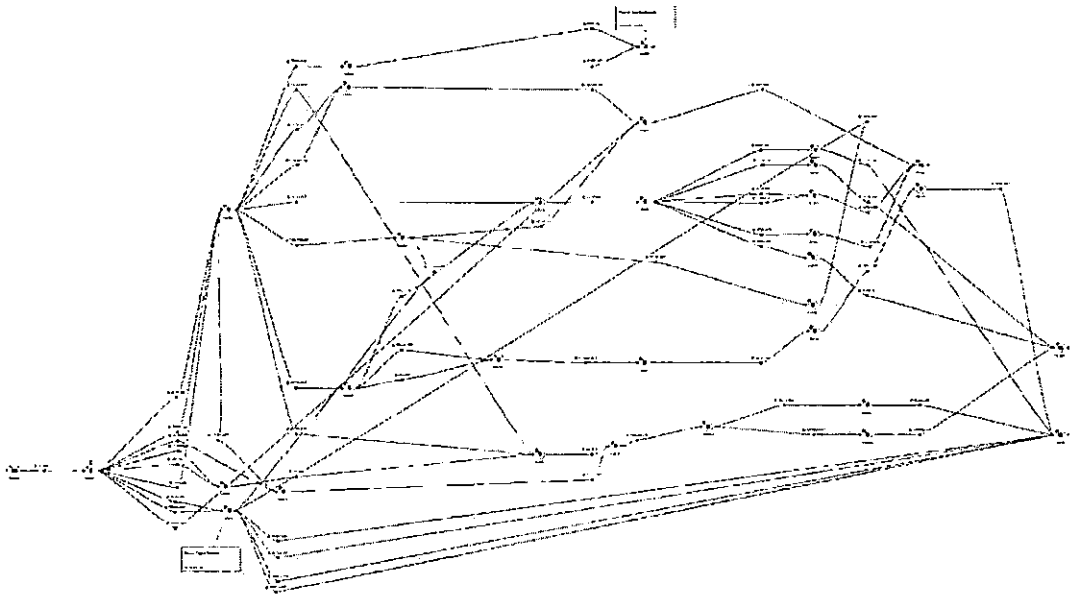
The on-chain tracing analysis revealed several methods employed by perpetrators to obscure the origin and flow of stolen assets.

1. **Structured Consolidation of Victim Transactions:** Smaller deposits from various victims were combined to form larger sums, making it difficult to trace individual origins. Several instances of funds consolidation were observed, as identified in the transaction graphs highlighting Pivot Wallets #1 and #2. These wallets obscure the original source of funds and facilitate layering to evade detection.

Tracing Graphs



Full Forensic Trace



Additional Pivot Tracing

V. WALLETS TO FREEZE

49. The blockchain addresses listed below are exchange-hosted deposit addresses associated with centralized cryptocurrency exchanges. Forensic blockchain tracing shows that these addresses received cryptocurrency traceable to Plaintiff's transfers. Such deposit addresses function as routing points through which assets are credited to user accounts maintained by the exchanges and therefore remain subject to restraint through the custodial control exercised by those exchanges.

Total Addresses to Freeze: [32]

Binance (6)

0x39e2023528f9d844a37e57a31f5d68a4963cd6f1

0x426de110cd4d80e5c9fdf82a3e84bf677299e6a7

0x924889649e0a886c8971251f080323491 1acaf69

0xa60e7b7326102ae789c36792c84aae26503590ea

0xda832c0af2a554ade4c02edc20cecd39d06e9405

0x44314413b3c95d1502d2d0a40af0b5a2d089a9f2

BitGet (1)

0x5221f03aa545012b4e5522cbf90fe6643f7c0dcb

Crypto.com (4)

0x373e32314091fb802d8a2470ae10bd6acc0f9193

0xd65c9409b59b96a9300ecbb3cfdd30d1eaa71897

0xef9dec0f94050c95ed47dbd7ea8cee464a3a58ee

0x748560126be09991b602df0fd4cb962b3d36e727

HTX (3)

0x4800281b5279436c1Da9351Cc47Ca4674eaC9ee5

0x779c77f64762e196ba6a95be745093dd305f67e0

0xb59a0a663756f36e9fe648e6ac5c4fe4123a8030

Kraken (5)

0xecba901bea6efa6674eb83944a6a8f1aa8f99cbe

0xf277d58b10705894608eaf4d24aa6a98696647bd

0xc82e9385bba254a9f9604b2eb752a359a266462a

0x7a13859703ec5cb5d0f621d80630d91c64d5ab21

0x1bd1fc2266cc3ba8a891845a21c4ff558cfe6567

MaskEx (1)

0x2322f132eed9aaa4355e697cadeb5f5882a49f34

Newton Canada (7)

0x63e7d31bbc152367760636d451b69e576a931761

0x9907c63c91d7b07f74bc45fb1b1d0eac0aa19c5e

0x653f3d52063074ae21131433747079cae713c2b3

0xcb52d1725fb8c2948a6e81d524e99f36c946153b

0x9fec3a05882247c98239c62951f90e21e999600e

0x354ce0d4f43a61ede5ed6125e7525ee13f33813a

0x28af85a5c33f2364b55378aa570deaef4f643566

OKX (3)

0x7285c5a958515e1b61bd042dd3d16af152fc5d1d

0x5262d9cfa573fe9010ca897545bdd6de671d95b8

0xc99bbf74fa693cb564e320e94cccf2d8296638df

Revolut (1)

0xf46ba229b6e8c5411ab9148af2485b7b2c841c76

Wealthsimple (1)

0x8f5a453d49c87abc35ad32af85945c0e82e79bcb

50. Based on my forensic blockchain analysis, it is my professional opinion that Plaintiff's cryptocurrency was transferred from her Coinbase account to Defendants' Intake Wallet, routed through Pivot Wallets and intermediary addresses, and deposited into exchange-hosted wallets controlled by or associated with Defendants.

51. It is further my professional opinion that these transactions reflect a structured process involving common wallet infrastructure, including shared Intake Wallets, Pivot Wallets,

and exchange-hosted deposit wallets, consistent with a coordinated cryptocurrency fraud scheme affecting multiple victims.

52. Based on my professional experience conducting blockchain forensic investigations, absent immediate injunctive relief the misappropriated cryptocurrency remains at substantial risk of being rapidly transferred through additional blockchain wallets or exchanges in a manner designed to obscure its origin and frustrate recovery. Cryptocurrency assets can be transferred through multiple blockchain wallets within seconds and across international jurisdictions beyond the reach of this Court.

53. Based on my experience investigating cryptocurrency exchanges and digital asset platforms, centralized exchanges such as Binance, BitGet, Crypto.com, HTX, Kraken, MaskEx, Newton Canada, OKX, Revolut, Wealthsimple maintain custody and control over deposit wallets associated with user accounts and have the technical ability to freeze or restrict withdrawals from those accounts when directed by court order.

I declare under penalty of perjury under the laws of the State of New York that the foregoing is true and correct. I affirm this 19th day of May, 2026 under the penalties of perjury under the laws of New York, which may include a fine or imprisonment, that the foregoing is true, except as to matters alleged on information and belief and as to those matters I believe it to be true, and I understand that this document may be filed in an action or proceeding in a court of law.

Executed this 19th day of May 2026.

DocuSigned by:
Maya Vick
452DFBCE7CEF49F...

Maya Vick