

AudiTrailGPT

Forensic Intelligence Report

Report Date: January 04, 2026

Source File: kaggle.txt

Executive Summary

Total log lines processed: 76

Successfully parsed alerts: **76**

Unmatched lines: 0

Total amount at risk: **\$501,972,768**

Analysis Engine: Llama-3.3-70B + Deterministic Symbolic Parser

Risk Indicators & Alert Distribution

Alert Type	Count	%	Amount per Alert	Total Amount
GATHER-SCATTER	39	51.3%	\$11,226	\$437,814
CYCLE	17	22.4%	\$132,713	\$2,256,121
FAN-IN	9	11.8%	\$1,155,546	\$10,399,914
STACK	6	7.9%	\$5,331	\$31,986
FAN-OUT	3	3.9%	\$84	\$252
SCATTER-GATHER	2	2.6%	\$10,228	\$20,456
TOTAL	76	100%		\$501,972,768

Complete Event Timeline

Date	Case ID	Alert Type	Amount
2022-09-01	FC000001	STACK	\$5,331
2022-09-01	FC000003	STACK	\$1,400
2022-09-01	FC000004	STACK	\$1,467
2022-09-01	FC000007	CYCLE	\$132,713
2022-09-01	FC000008	CYCLE	\$18,264
2022-09-01	FC000019	FAN-IN	\$1,155,546
2022-09-01	FC000020	FAN-IN	\$1,104,862
2022-09-01	FC000021	FAN-IN	\$1,392,590
2022-09-01	FC000028	CYCLE	\$90,469,674
2022-09-01	FC000029	CYCLE	\$90,469,674
2022-09-01	FC000033	GATHER-SCATTER	\$11,226
2022-09-01	FC000038	GATHER-SCATTER	\$357,414
2022-09-01	FC000058	SCATTER-GATHER	\$10,228
2022-09-01	FC000060	FAN-OUT	\$84
2022-09-01	FC000063	GATHER-SCATTER	\$4,151
2022-09-02	FC000005	STACK	\$16,898
2022-09-02	FC000009	CYCLE	\$14,567
2022-09-02	FC000010	CYCLE	\$114,329
2022-09-02	FC000022	FAN-IN	\$118,642
2022-09-02	FC000023	FAN-IN	\$763,621
2022-09-02	FC000030	CYCLE	\$77,206,819
2022-09-02	FC000034	GATHER-SCATTER	\$11,440
2022-09-02	FC000035	GATHER-SCATTER	\$2,317
2022-09-02	FC000036	GATHER-SCATTER	\$2,710
2022-09-02	FC000037	GATHER-SCATTER	\$2,937
2022-09-02	FC000039	GATHER-SCATTER	\$1,474,382
2022-09-02	FC000061	FAN-OUT	\$2,567
2022-09-02	FC000064	GATHER-SCATTER	\$2,513
2022-09-02	FC000065	GATHER-SCATTER	\$36,468,598
2022-09-02	FC000066	GATHER-SCATTER	\$14,180
2022-09-03	FC000002	STACK	\$5,602
2022-09-03	FC000006	STACK	\$17,607
2022-09-03	FC000011	CYCLE	\$14,567

2022-09-03	FC000012	CYCLE	\$13,629
2022-09-03	FC000013	CYCLE	\$97,481
2022-09-03	FC000031	CYCLE	\$90,469,674
2022-09-03	FC000040	GATHER-SCATTER	\$714,621
2022-09-03	FC000067	GATHER-SCATTER	\$13,650
2022-09-03	FC000068	GATHER-SCATTER	\$8,370
2022-09-03	FC000069	GATHER-SCATTER	\$7,525,208
2022-09-04	FC000014	CYCLE	\$14,054
2022-09-04	FC000015	CYCLE	\$13,718
2022-09-04	FC000024	FAN-IN	\$19,082
2022-09-04	FC000032	CYCLE	\$90,469,674
2022-09-04	FC000041	GATHER-SCATTER	\$585,445
2022-09-04	FC000070	GATHER-SCATTER	\$3,052
2022-09-05	FC000016	CYCLE	\$12,908
2022-09-05	FC000025	FAN-IN	\$1,306,642
2022-09-05	FC000026	FAN-IN	\$1,409,305
2022-09-05	FC000027	FAN-IN	\$324,388
2022-09-05	FC000042	GATHER-SCATTER	\$1,064,274
2022-09-05	FC000043	GATHER-SCATTER	\$1,221,106
2022-09-05	FC000044	GATHER-SCATTER	\$1,416,050
2022-09-05	FC000071	GATHER-SCATTER	\$4,664
2022-09-05	FC000072	GATHER-SCATTER	\$11,290
2022-09-05	FC000073	GATHER-SCATTER	\$9,324
2022-09-06	FC000017	CYCLE	\$10,636
2022-09-06	FC000018	CYCLE	\$1,378,736
2022-09-06	FC000059	SCATTER-GATHER	\$10,341
2022-09-06	FC000062	FAN-OUT	\$9,352
2022-09-06	FC000074	GATHER-SCATTER	\$653
2022-09-06	FC000075	GATHER-SCATTER	\$176
2022-09-06	FC000076	GATHER-SCATTER	\$9
2022-09-07	FC000045	GATHER-SCATTER	\$209,953
2022-09-07	FC000046	GATHER-SCATTER	\$975,071
2022-09-07	FC000047	GATHER-SCATTER	\$23,009
2022-09-09	FC000048	GATHER-SCATTER	\$14,421
2022-09-09	FC000049	GATHER-SCATTER	\$1,131,484
2022-09-10	FC000050	GATHER-SCATTER	\$8,362

2022-09-10	FC000051	GATHER-SCATTER	\$18,913
2022-09-11	FC000052	GATHER-SCATTER	\$1,102
2022-09-12	FC000053	GATHER-SCATTER	\$2,549
2022-09-12	FC000054	GATHER-SCATTER	\$9,263
2022-09-12	FC000055	GATHER-SCATTER	\$4,829
2022-09-13	FC000056	GATHER-SCATTER	\$44,143
2022-09-13	FC000057	GATHER-SCATTER	\$3,237

Detailed Forensic Analysis (Llama-3.3 Generated)

1. Executive Summary and Key Findings

The investigation has uncovered a complex network of financial transactions involving cross-border entities, with a total of **76 alerts** detected over a period of **13 days**. The total amount at risk is estimated to be **\$501,972,768**. The alerts are categorized into several types, including **STACK**, **CYCLE**, **FAN-IN**, **FAN-OUT**, **GATHER-SCATTER**, and **SCATTER-GATHER**. The most significant alerts are related to **CYCLE** and **FAN-IN** transactions, with amounts ranging from **\$10636** to **\$90469674**.

- **High-Risk Transactions:** Multiple high-risk transactions have been detected, including **CYCLE** and **FAN-IN** transactions with large amounts.
- **Cross-Border Entities:** All transactions involve cross-border entities, indicating potential money laundering or terrorist financing activities.
- **Complex Network:** The transactions suggest a complex network of entities and accounts, making it challenging to identify the primary beneficiaries or sinks.

Key Findings:

2. Comprehensive Event Timeline

The following table presents a detailed timeline of the detected events:

3. Threat Assessment and Risk Indicators

- **Large Transaction Amounts:** Transactions with large amounts, such as **\$90469674**, indicate a high risk of money laundering or terrorist financing.
- **Cross-Border Entities:** The involvement of cross-border entities in all transactions increases the risk of money laundering or terrorist financing.
- **Complex Transaction Patterns:** The detection of complex transaction patterns, such as **CYCLE** and **FAN-IN** transactions, suggests a high risk of money laundering or terrorist financing.
- **High-Risk:** Transactions with large amounts and complex patterns, such as **CYCLE** and **FAN-IN** transactions.
- **Medium-Risk:** Transactions with moderate amounts and less complex patterns, such as **STACK** and **GATHER-SCATTER** transactions.
- **Low-Risk:** Transactions with small amounts and simple patterns, such as **FAN-OUT** transactions.

The following risk indicators have been identified: ### Risk Levels:

4. In-Depth Pattern and Trend Analysis

- **CYCLE Transactions:** These transactions involve the movement of funds between entities in a cyclical pattern, indicating a potential money laundering scheme.

- **FAN-IN Transactions:** These transactions involve the movement of funds from multiple entities to a single entity, indicating a potential money laundering scheme.
- **GATHER-SCATTER Transactions:** These transactions involve the movement of funds from a single entity to multiple entities, indicating a potential money laundering scheme.
- **Frequency Analysis:** The frequency of transactions suggests a consistent pattern of activity, indicating a potential ongoing money laundering scheme.
- **Amount Analysis:** The analysis of transaction amounts suggests a range of amounts, from small to large, indicating a potential money laundering scheme.

The analysis of the transaction patterns and trends reveals: ### Pattern Analysis:

5. Financial Impact and Exposure Assessment

The total amount at risk is estimated to be **\$501,972,768**. The financial impact of these transactions could be significant, with potential losses for financial institutions and damage to the integrity of the financial system.

- **Direct Exposure:** The direct exposure is estimated to be **\$501,972,768**, which is the total amount of the detected transactions.
- **Indirect Exposure:** The indirect exposure is potentially much larger, as the detected transactions may be part of a larger money laundering scheme.

Exposure Assessment:

6. Money Laundering Typologies and Red Flags

- **Structuring:** The use of multiple transactions to avoid detection, such as **STACK** transactions.
- **Layering:** The use of complex transaction patterns to conceal the origin of funds, such as **CYCLE** and **FAN-IN** transactions.
- **Smurfing:** The use of multiple entities to move funds, such as **GATHER-SCATTER** transactions.
- **Unusual Transaction Patterns:** Transactions that do not follow normal patterns, such as **CYCLE** and **FAN-IN** transactions.
- **Large Transaction Amounts:** Transactions with large amounts, such as **\$90469674**.
- **Cross-Border Entities:** The involvement of cross-border entities in all transactions.

The detected transactions match several known money laundering typologies, including: ### Red Flags:

7. Granular Investigation Recommendations

- **Entity Analysis:** Analyze the entities involved in the detected transactions to identify potential relationships and connections.
- **Transaction Analysis:** Analyze the transactions in more detail to identify potential patterns and trends.

- **Network Analysis:** Analyze the network of entities and transactions to identify potential money laundering schemes.
- **Gather Additional Information:** Gather additional information about the entities and transactions involved.
- **Conduct Further Analysis:** Conduct further analysis of the transactions and entities to identify potential patterns and trends.
- **Develop a Case Theory:** Develop a case theory based on the analysis and investigation.

The following recommendations are made for further investigation: ### Next Steps:

