Pig Butchering Network Analysis – Summary Report

Pig Butchering Network Analysis

By Rashad Ferguson

Project Overview

Pig butchering is more than a scam—it's a coordinated financial operation. This project offers a forensic model of how these schemes function at scale, helping regulators and institutions understand the velocity, structure, and blind spots in current anti-money laundering systems.

Problem Framing

The Problem:
Pig butchering scams represent a rapidly evolving form of financial fraud that combines romance scam tactics with cryptocurrency investment schemes. These operations, which originated in Southeast Asia, have caused billions in losses globally by exploiting victims through elaborate social engineering campaigns that can span months. The scammers build trust through fake romantic or friendship connections before convincing victims to invest in fraudulent cryptocurrency platforms.

Why This Matters:
The scale and sophistication of these networks pose significant challenges for financial institutions, law enforcement, and potential victims. In 2023 alone, the FBI reported over $3.3 billion in cryptocurrency investment fraud losses, with pig butchering schemes representing a substantial portion. Beyond financial damage, these scams cause severe emotional trauma and often target vulnerable populations including the elderly and socially isolated individuals.

Analysis Focus:
This analysis examines the network structure and operational patterns of pig

butchering scams by analyzing simulated transaction patterns and network behaviors. The investigation aims to identify key indicators, network vulnerabilities, and potential intervention points that could help financial institutions and law enforcement agencies detect and prevent these scams more effectively.

Scope:
The analysis covers global operations with emphasis on Southeast Asian networks, focusing on money flow patterns, cryptocurrency conversion strategies, and temporal laundering behaviors. While comprehensive in its technical approach, this study uses simulated data to model real-world patterns observed in documented cases.

Goals & Audience

This analysis aims to create a data-driven model that reveals operational patterns in pig butchering schemes and identifies detection opportunities. It is designed for financial regulators, AML compliance teams, law enforcement agencies, and cybersecurity professionals who need actionable intelligence on modern laundering methods.

Key Findings

- **Regional Losses:** Southeast Asia accounts for $44B, or 58% of total annual losses.
- **Crypto Behavior:** Tether dominates laundering volume with $15.2B in conversions.
- **Speed of Laundering:** 93% of illicit funds are moved within 48 hours.
- **Banking Exposure:** Over 140M accounts linked to $260B+ in suspect flows.
- **Effectiveness:** Syndicates successfully move 89% of targeted assets.

Methodology & Tools

- **Framework:** Central money_laundering_data Python structure simulating the crime ecosystem

- **Analysis:** NetworkX centrality metrics, Sankey flows, conversion heatmaps, temporal models
- **Technologies:** Python, Pandas, Matplotlib, Seaborn, Plotly
- **Outputs:** PNG/HTML charts and JSON summaries

Impact

This model provides actionable insights for institutions and policymakers aiming to detect, disrupt, and dismantle modern laundering systems. It highlights enforcement blind spots, conversion choke points, and banking vulnerabilities exploited by transnational financial crime.