

■ CLASSIFICATION: UNCLASSIFIED // OPEN-SOURCE ■

LANDRY INDUSTRIES INC. · MARIE LANDRY'S SPY SHOP
INTELLIGENCE DOSSIER

Banking Blind Spots

Systemic AML Failure in Global Banking Infrastructure

DOSSIER REF: LI-AML-2026-001
AUTHOR: Marie-Soleil Seshat Landry, CEO — Landry Industries Inc.
DATE: April 2026 · Moncton, New Brunswick, Canada
ORCID: 0009-0008-5027-3337 · marielandryspyshop.com

Full OSINT Analysis · Illicit Financial Flow Mapping · Detection System Architecture · Working Prototype Code

This dossier analyzes systemic anti-money laundering (AML) failures within global banking infrastructure, using illicit financial flows linked to fentanyl distribution as a case lens, with enforcement exposure involving TD Bank. All analysis is based on publicly available sources (OSINT).

01. EXECUTIVE SUMMARY

This dossier analyzes systemic anti-money laundering (AML) failures within global banking infrastructure. The case anchor is illicit financial flow activity linked to fentanyl distribution networks, with enforcement exposure documented at TD Bank.

Core Finding:

The observed failures are not instances of isolated misconduct. They represent a predictable, structural breakdown of financial surveillance systems operating under adversarial conditions. Banks do not originate criminal activity — but they enable its scaling when detection architecture fails to adapt.

The critical asymmetry: criminal networks operate as adaptive, decentralized systems. Financial compliance systems do not.

02. PROBLEM ANALYSIS

Structural Weaknesses

- AML systems are **compliance-driven**, not **intelligence-driven**

- Criminal networks operate as adaptive, decentralized systems — banks analyze accounts in isolation
- Detection is largely **reactive**, not real-time
- Institutional incentives prioritize transaction throughput over risk mitigation
- Alert systems generate high false-positive rates, diluting genuine signal

Systemic Failure Points

FAILURE POINT	OPERATIONAL CONSEQUENCE
Alert Overload	High false-positive rates dilute genuine signals — analysts miss real patterns
Siloed Intelligence	Accounts analyzed individually; criminal network topology invisible
Delayed Reporting	Lag between suspicious activity and formal reporting allows layering to complete
Cross-Border Gap	Weak inter-jurisdictional data integration enables offshore movement
Incentive Misalignment	Revenue and throughput goals conflict with aggressive AML enforcement

03. CASE ANCHOR: TD BANK

TD Bank serves as the primary institutional case anchor for this analysis. Documented deficiencies span approximately 2014 to 2023 and include failure to detect structuring patterns, weak escalation of suspicious activity reports (SARs), and confirmed exposure to drug-linked laundering flows.

Interpretation: This case does not represent an outlier. It represents a systemic detection failure at scale — a visible instance of a vulnerability that exists across global banking infrastructure.

- AML program deficiencies documented over approximately **9-year window** (2014–2023)
- Failure to detect or escalate sub-threshold structuring activity
- Exposure to fentanyl distribution-linked financial flows
- Enforcement action: penalty imposed, remediation required

04. ILLICIT FINANCIAL FLOW MODEL

Four-stage laundering architecture — Placement → Layering → Integration — mapped against observable banking system indicators.

STAGE	NAME	MECHANISM	INDICATORS
01	Cash Generation	Street-level distribution networks generate bulk untracked cash via fentanyl markets	No bank-side visibility at this stage
02	Placement	Deposits structured below \$10,000 reporting thresholds across multiple branches; intermediary 'mules' used to segment transaction trails	Repeated sub-threshold deposits; branch hopping; economic profile inconsistency

STAGE	NAME	MECHANISM	INDICATORS
03	Layering	Rapid inter-account transfers; shell company routing; cross-border wire movement to obscure beneficial ownership	Deposit-to-transfer velocity; shared counterparty endpoints; offshore destination flags
04	Integration	Funds re-enter legitimate economy via real estate, business investment, or financial assets	Transaction size normalization; reduced velocity; increased counterparty diversity

05. DETECTABLE PATTERNS

These systems are not invisible. Laundering activity leaves repeatable, detectable signals across multiple behavioral dimensions.

RULE	TRIGGER CONDITION	RISK SCORE
Structuring	3+ deposits < \$10,000 within rolling 7-day window, same account	+30 pts
Velocity	Deposit → outbound transfer within 24 hours	+25 pts
Branch Hopping	3+ deposit branches in 30 days, inconsistent geography	+20 pts
Hub Convergence	Multiple accounts route transfers to single counterparty node	+35 pts
Profile Mismatch	Transaction volume inconsistent with declared economic activity	+20 pts

Risk Score Threshold: Accounts scoring ≥ 30 trigger automated SAR review. Accounts scoring ≥ 55 trigger priority escalation.

06. DETECTION SYSTEM DESIGN

Core Detection Logic

- **Structuring Rule:** IF deposits < 10,000 AND count ≥ 3 within rolling window → FLAG (+30)
- **Velocity Rule:** IF deposit → transfer within 24 hours → FLAG (+25)
- **Network Rule:** IF multiple accounts converge on shared endpoint node → FLAG cluster (+35)
- **Profile Rule:** IF transaction volume exceeds economic profile baseline → FLAG (+20)

07. IMPLEMENTATION — WORKING PROTOTYPE

Three-module prototype: synthetic dataset generation, rule-based detection engine, network graph intelligence layer.

Module 1 — Synthetic Transaction Dataset

```
import pandas as pd, random
from datetime import datetime, timedelta

accounts = [f'A{i}' for i in range(1, 51)]
branches = [f'B{i}' for i in range(1, 6)]
data = []
start = datetime(2026, 1, 1)

# Normal users (A1-A30): low-value, varied deposits
for acc in accounts[:30]:
    for i in range(20):
        data.append({'account_id': acc, 'type': 'deposit',
                    'amount': random.randint(100, 3000),
                    'timestamp': start + timedelta(days=i),
                    'branch_id': random.choice(branches), 'counterparty': None})

# Laundering accounts (A31-A40): structuring + rapid transfer
for acc in accounts[30:40]:
    for i in range(5):
        data.append({'account_id': acc, 'type': 'deposit',
                    'amount': random.randint(8000, 9900),
                    'timestamp': start + timedelta(days=i),
                    'branch_id': random.choice(branches), 'counterparty': None})
        data.append({'account_id': acc, 'type': 'transfer',
                    'amount': random.randint(8000, 9900),
                    'timestamp': start + timedelta(days=i, hours=5),
                    'branch_id': None, 'counterparty': 'HUB1'})

df = pd.DataFrame(data)
df.to_csv('transactions.csv', index=False)
```

Module 2 — Rule-Based Detection Engine

```
import pandas as pd

df = pd.read_csv('transactions.csv', parse_dates=['timestamp'])
df = df.sort_values(by=['account_id', 'timestamp'])
alerts = {}

for account, group in df.groupby('account_id'):
    score = 0
    deposits = group[group['type'] == 'deposit']

    # Rule 1: Structuring
    if len(deposits[deposits['amount'] < 10000]) >= 3:
        score += 30

    # Rule 2: Velocity (deposit → transfer within 24h)
    for i in range(len(group) - 1):
        if (group.iloc[i]['type'] == 'deposit' and
```

```
group.iloc[i+1]['type'] == 'transfer')):
    delta = group.iloc[i+1]['timestamp'] - group.iloc[i]['timestamp']
    if delta.total_seconds() < 86400:
        score += 25
    break
if score > 0:
    alerts[account] = score
print('=== RISK SCORES ===')
for acc, score in sorted(alerts.items(), key=lambda x: -x[1]):
    tier = 'PRIORITY' if score >= 55 else 'REVIEW'
    print(f'{acc} score={score} [{tier}])
```

Module 3 — Network Graph Intelligence

```
import pandas as pd
import networkx as nx
import matplotlib.pyplot as plt

df = pd.read_csv('transactions.csv')
G = nx.DiGraph()

for _, row in df.iterrows():
    if row['type'] == 'transfer' and pd.notna(row['counterparty']):
        G.add_edge(row['account_id'], row['counterparty'],
                    weight=row['amount'])

# Identify hub nodes (high in-degree)
hubs = [n for n, d in G.in_degree() if d >= 3]
print(f'Hub nodes detected: {hubs}')

plt.figure(figsize=(12, 8))
pos = nx.spring_layout(G, seed=42)
node_colors = ['#C0392B' if n in hubs else '#C9A84C' for n in G.nodes()]
nx.draw(G, pos, with_labels=True, node_color=node_colors,
        edge_color='#8A9BB0', node_size=500, font_size=7)
plt.title('Transaction Network — Hub Detection')
plt.savefig('network_graph.png', dpi=150, bbox_inches='tight')
plt.show()
```

08. STRATEGIC INSIGHT

The illicit financial system described in this dossier is **predictable**, **pattern-based**, and **detectable**. The failure to detect it is not primarily a technical problem — it is an architectural and operational one.

Current AML architecture is built for regulatory compliance. What is required is intelligence-grade adversarial detection.

Recommended Capability Upgrades

- Shift from account-level to **network-level** transaction analysis
- Implement **real-time velocity monitoring** with automated escalation
- Deploy **graph analytics** to surface hub convergence patterns

- Integrate **economic profile baselines** per account segment
- Establish **cross-institution data sharing** frameworks under regulatory mandate
- Adopt **adversarial simulation** (red team AML) to test detection coverage

09. FINAL CONCLUSION

The framing of fentanyl-linked bank enforcement actions as isolated scandals is a misdiagnosis. The TD Bank case is illustrative, not exceptional.

The real issue is systemic AML failure within global financial infrastructure — a structural vulnerability that exists wherever compliance-driven detection confronts intelligence-grade adversarial adaptation.

This dossier provides the analytical foundation, the detection logic, and working prototype code to begin closing that gap.

Next steps: (A) Deploy prototype against live or synthetic datasets. (B) Extend network module to multi-hop graph traversal. (C) Integrate with Streamlit dashboard for operational visualization. (D) Publish findings via Zenodo under Landry Industries ORCID.

— Marie-Soleil Seshat Landry
CEO & Founder, Landry Industries Inc.
Marie Landry's Spy Shop · marielandryspyshop.com
ORCID: 0009-0008-5027-3337