MULE ANALYSIS

PROJECT FRAMING & OBJECTIVES

5W1H Core Questions

WHO — บัญชีแบบใดเสี่ยงเป็นม้ามากที่สุด? → วิเคราะห์ risk_segment, kyc_status, employment_status, account_age → สมมติฐาน: Burner = บัญชีใหม่ <30 วัน, Sleeper = บัญชีเก่าถูก recruit, Pending KYC + Salaried/Student = เป้าหมายหลัก

WHAT — สัญญาณใดแยกธุรกรรมม้าได้ดีที่สุด? → ทดสอบ amount_z_score (ขนาดยอด) vs burst_score (ความถี่) → สมมติฐาน: ยอด หรือ ความถี่ คือสัญญาณหลัก?

WHERE — ช่องทางใดเสี่ยงสูง? → เปรียบเทียบ Mule Rate ต่อ transfer_method → ขอบเขต: Exploratory — Synthetic Data ไม่มีอคติเชิงช่องทาง ใช้เป็น Baseline สำหรับข้อมูลจริง

WHEN — ธุรกรรมม้ากระจุกตัวช่วงเวลาใด? → วิเคราะห์ Hourly Distribution → ขอบเขต: Supporting Signal ประกอบ Compound Rule — ไม่ใช่ Standalone Rule

WHY — เหตุใด Pass-through จึงเป็นสัญญาณสำคัญ? → เชื่อมโยง in_out_ratio_7d + dwell_time_minutes — บัญชีม้าคือ "ท่อ" (Pipe) ไม่ใช่ "อ่าง" (Reservoir)

HOW — บัญชีม้าเคลื่อนย้ายเงินอย่างไร? → วิเคราะห์ Topology: Victim → Sleeper → Burner(s) → Crypto Wallet → คำถามย่อย: Burst ใน Hop 2 สูงกว่าปกติกี่เท่า และ Compound Rule (Burst + Dwell + First-Time Payee) คัดกรองได้แค่ไหน?

SMART OBJECTIVES

S — Specific: วิเคราะห์พฤติกรรมบัญชีม้า (Burner/Sleeper) ผ่านยอดเงิน, ความถี่, อายุบัญชี, Pass-through — เพื่อสกัด Rule-based Detection ที่ใช้งานได้จริง

M — Measurable (ต้องบรรลุทุก Target):

Behavioral Signals:

- **Dwell Time:** ≥ 90% ของการทำธุรกรรมบัญชีม้า (Hop 2–3) มี Dwell < 5 นาที
- **In/Out Ratio 7 วัน:** Mule Rate ในกลุ่ม Ratio 0.9–1.0 มี Lift ≥ 2.0x
- **Burst Score:** ≥ 80% ของ Hop 2 มี Burst ≥ 3
- **Account Age:** Burner ทุกบัญชี มี Age < 30 วัน
- **Hourly Pattern:** สัดส่วนบัญชีม้าในช่วง 00:00–06:00 มี Lift ≥ 2.0x

Detection System:

- **Compound Rule:** Mule Precision ≥ 50% (Lift ≥ 50x จาก Baseline 1%) และ FPR ≤ 0.05%

A — Achievable: **Synthetic Data ~20,000** ธุรกรรม จาก 1,000 บัญชี, 20 Mule Rings แบบ Non-overlapping ที่สะท้อนพฤติกรรมจริง

R — Relevant: ใช้เป็น **Rule-based Risk Indicators** คัดกรองบัญชีต้องสงสัยได้ทันที โดยไม่ต้องรอ ML Model

T — Time-bound: Data Pipeline + Feature Engineering + EDA Insight ภายใน Final Submission

DATA DICTIONARY

STAR SCHEMA — DENORMALIZED INTO ONE BIG TABLE (OBT) FOR BI

Table 1 — dim_customers

Field	Type	Description
customer_id	String (PK)	Unique customer identifier
age	Integer	Customer age (18–75)
employment_status	String	Salaried / Student / Unemployed / Self-Employed
kyc_status	String	Verified / Pending / Rejected
risk_segment	String	Low / Medium / High

Table 2 — dim_accounts

Field	Type	Description
account_id	String (PK)	Unique account identifier
account_creation_date	Timestamp	When account was opened
initial_deposit	Float	Starting balance (THB)
is_mule_flag	Boolean	Ground truth mule label
mule_type	String	Burner / Sleeper / None

Table 3 — fact_transactions (key fields only)

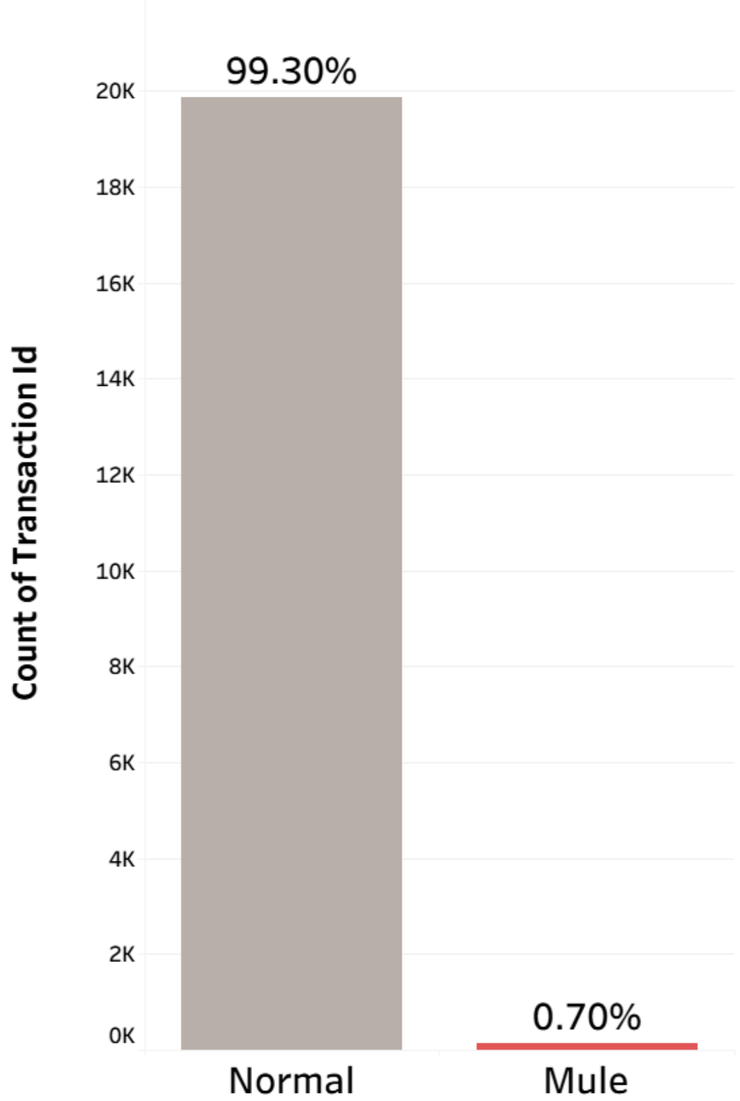
Field	Type	Description
transaction_id	String (PK)	Unique transaction identifier
amount	Float	Transfer amount (THB)
transfer_method	String	Mobile App / Web / API / ATM
is_mule_tx	Boolean	Target variable — is this a mule transaction?
dwell_time_minutes	Float	Minutes from last credit to this debit — pass-through signal
burst_score	Integer	Outgoing transfers in last 1 hour — velocity signal
amount_z_score	Float	Deviation from sender's historical average — anomaly signal
in_out_ratio_7d	Float	Credits/debits ratio over 7 days — pass-through strength
account_age_days	Integer	Sender account age at transaction time — burner signal

Full schema: 25 fields across 3 tables — see GitHub README for complete field definitions

EDA Overview — Dataset Characteristics Before Analysis

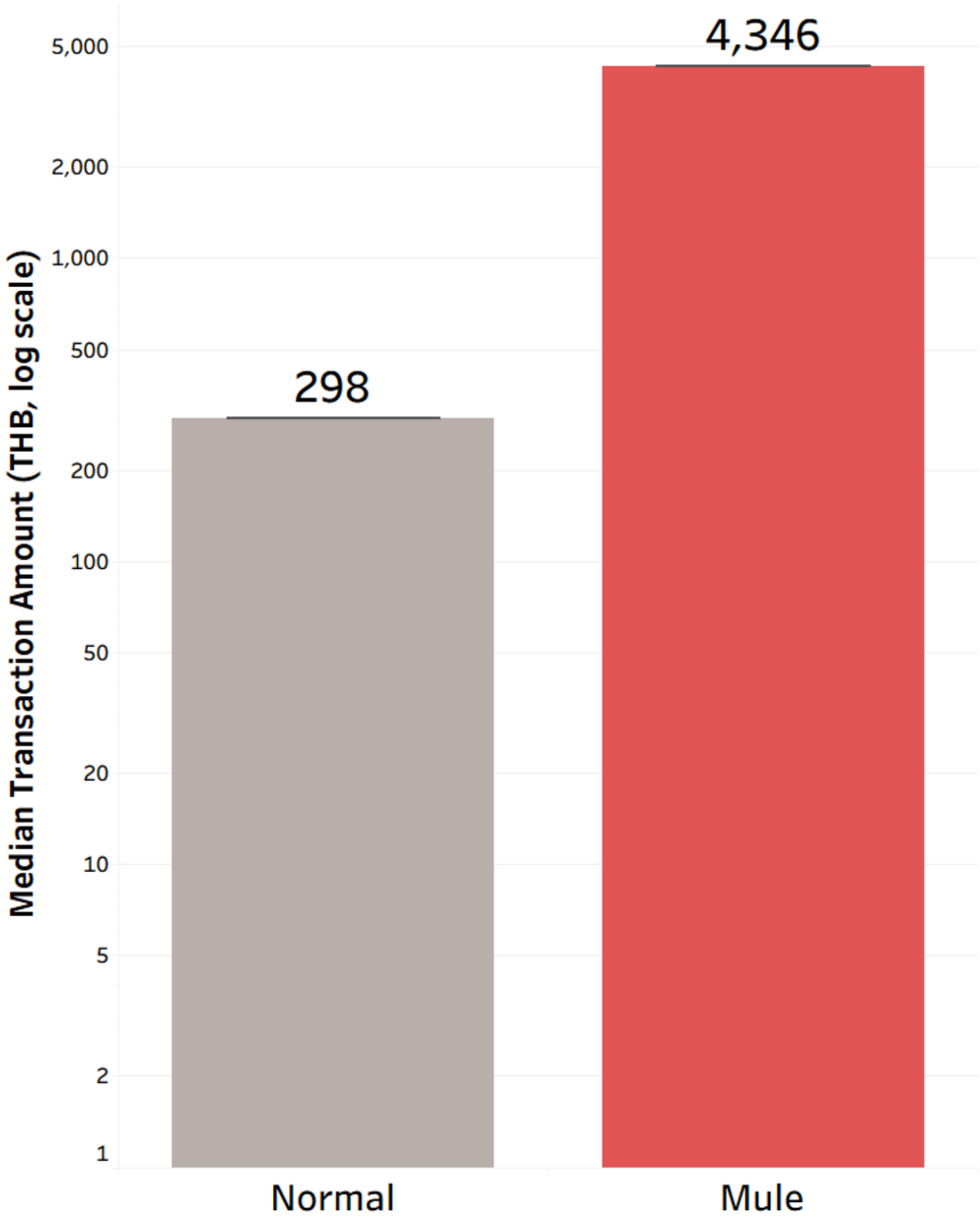
Class Distribution

Mule transactions = 0.7% of dataset — severe class imbalance requiring normalized analysis



Amount Distribution (Log Scale)

Mule median = 4,346 THB — 15× higher than Normal (298 THB)



Feature Signal by Class

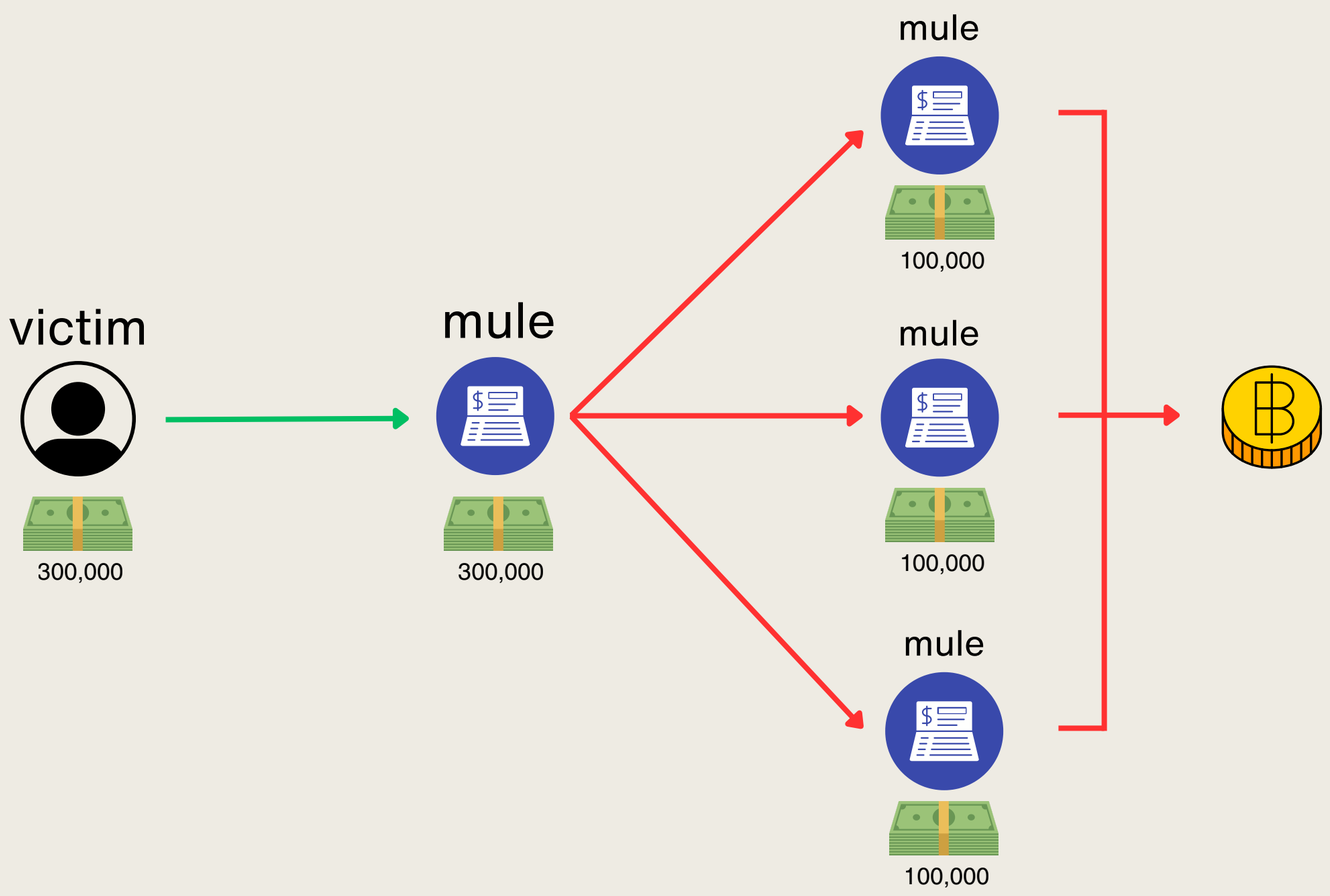
Mules move money in 5 min vs 7,259 min normal — accounts are 2.7× newer (168 vs 458 days)

	Normal	Mule
Median Account Age	458	168
Median Dwell Time	7,259	5

SYNTHETIC DATA GENERATION APPROACH

SIMULATING REAL-WORLD BANKING TRAFFIC

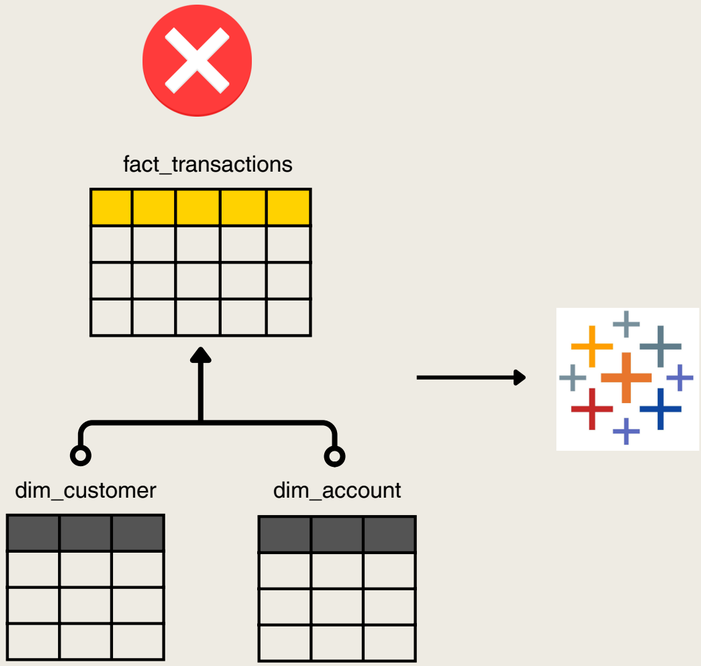
- **Stateful Simulation, Not Random Noise:** Modeled 180 days of chronological financial activity across 1,000 retail accounts.
- **Normal Behavioral Engine:** Legitimate accounts follow mathematical distributions mimicking daily life (e.g., monthly salary deposits, routine weekly expenses).
- **Injecting the "Smurf Ring":** Programmed highly specific, multi-hop anomaly events to represent Thai mule networks.
- **The Attack Path:** Victim Transfer ➔ "Sleeper" Account ➔ Split to "Burner" Accounts ➔ Rapid External Exit (Crypto/Other Bank).

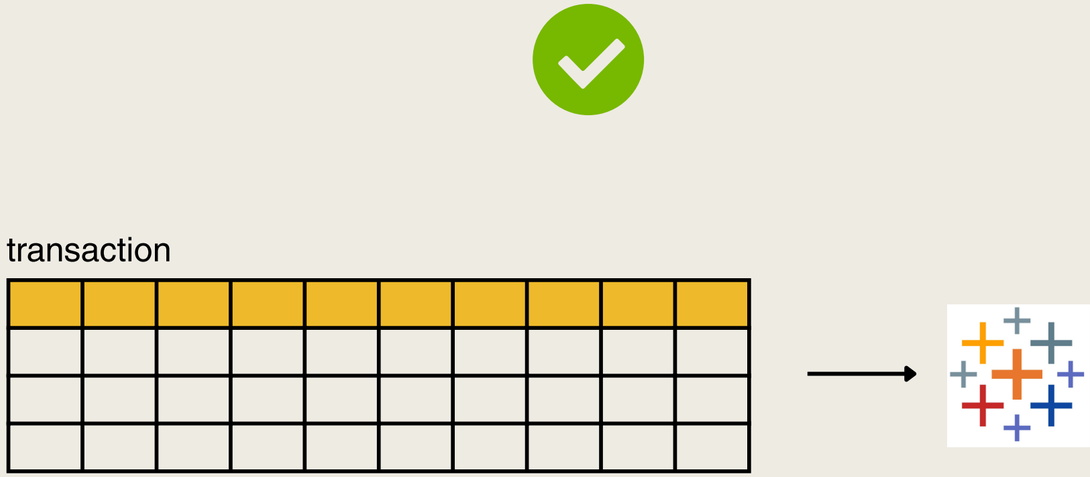


DATA ARCHITECTURE & SCHEMA

THE "ONE BIG TABLE" (OBT) SCHEMA

- **Optimized for Business Intelligence:** Bypassed a traditional, multi-table Star Schema in favor of a denormalized, 15-column flat table (OBT).
- **Pre-Calculated ETL:** Shifted heavy computational loads (sliding windows, state tracking) into the Python data pipeline rather than the BI tool.
- **Dashboard Ready:** This architecture eliminates complex SQL joins at the presentation layer, enabling zero-latency filtering and aggregation in tools like Tableau or Power BI.



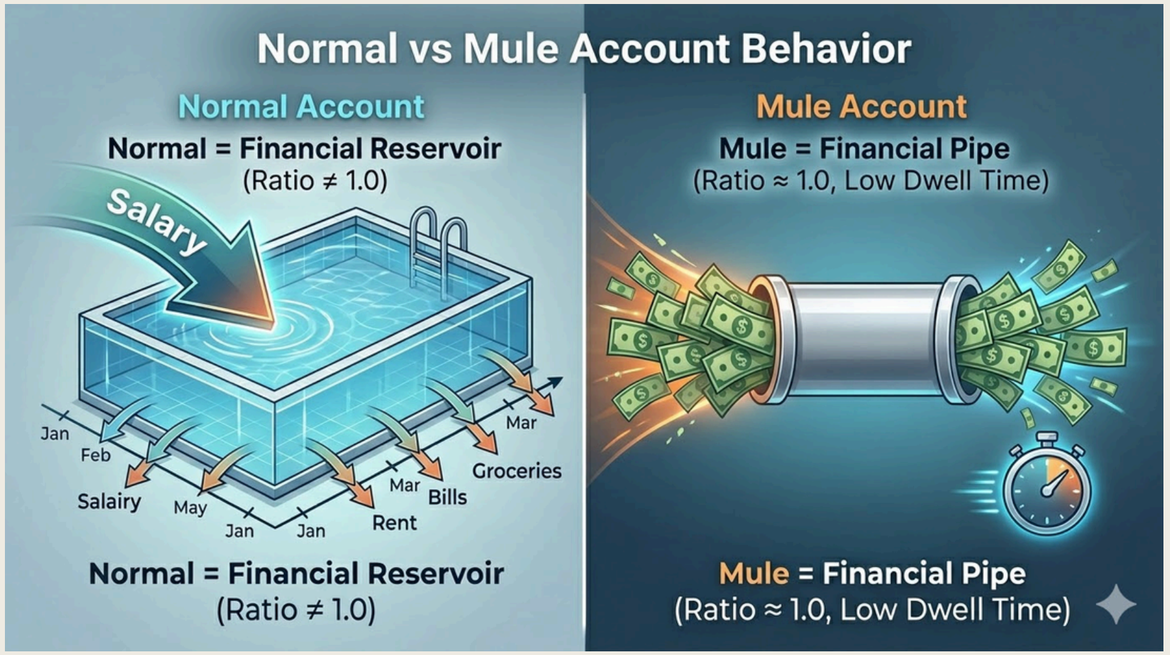


ENGINEERING BEHAVIORAL KPIS

RAW DATA IS NOT ENOUGH: ENGINEERED FEATURES

Standard, static rules fail to catch mule accounts. We engineered derived metrics to expose "pass-through" velocity:

- **Dwell Time (Minutes):** Time elapsed between an account receiving a credit and sending a debit. (Catches rapid exit transfers).
- **7-Day In/Out Ratio:** The proportion of credits vs. debits over a rolling week. (Mule accounts hover almost exactly at 1.0).
- **Amount Z-Score:** Calculates the standard deviation of a transaction against the user's specific historical spending habits.



DATA QUALITY (DQ) LAYER - IDENTIFICATION

REAL-WORLD DATA IS DIRTY: THE DQ AUDIT

While our generated data is clean, a production pipeline must actively check for system noise before analysis:

- **Invalid Data:** Catching orphaned sender_account_ids or timezone mismatches (e.g., transaction dates in the future).
- **Noise & System Glitches:** Identifying missing device_ids from legacy system migrations or exact duplicate rows caused by double-firing APIs.
- **Outliers vs. Anomalies:** Using statistical bounds to distinguish a legitimate high-value outlier (e.g., buying a car) from a high-velocity scam outlier.

transaction_id	sender_account_id	receiver_account_id	amount	transaction_timestamp	transfer_method	is_mule_tx	sender_balance_before_tx	receiver_balance_before_
TXN_004398	ACC_0070	ACC_0143	1,029.06	2025-09-18 05:20:34	Mobile App	false	1,961.21	1,048.06
TXN_006418	ACC_0625	ACC_0596	429.26	2025-09-18 05:33:39	Mobile App	false	3,725.53	384.14
TXN_013459	ACC_0947	ACC_0336	1,367.84	2025-09-18 05:37:02	Mobile App	false	637.37	1,962.98
TXN_017300	ACC_0147	ACC_0932	707.38	2025-09-18 05:47:10		false	1,183.68	3,677.65
TXN_006405	ACC_0415	ACC_0173	369.15	2025-09-18 05:56:23	Mobile App	false	4,475.25	184.13
TXN_000433	ACC_0398	ACC_0016	1,463.10	2025-09-18 06:41:25	Mobile App	false	3,667.56	1,589.36
TXN_014753	ACC_0768	ACC_0583	-500	2025-09-18 06:43:13	Mobile App	false	2,759.98	857.02
TXN_016787	ACC_0276	ACC_0833	1,481.28	2025-09-18 06:44:35	Mobile App	false	3,541.66	3,844.31
TXN_010375	ACC_0768	ACC_0723	1,190.96	2025-09-18 06:49:04	API	false	2,731.09	4,615.72
TXN_010591	ACC_0659	ACC_0634	126.76	2025-09-18 06:50:44	Web	false	2,811.74	2,620.16
TXN_010591	ACC_0659	ACC_0634	126.76	2025-09-18 06:50:44	Web	false	2,811.74	2,620.16
TXN_007655	ACC_0065	ACC_0321	1,213.11	2025-09-18 07:04:19	Mobile App	false	2,393.69	3,699.04
TXN_007201	ACC_0096	ACC_0870	1,307.78	2025-09-18 07:43:18	Mobile App	false	981.20	4,840.62
TXN_018821	ACC_0428	ACC_0709	100.78	2025-09-18 08:02:14	ATM	false	3,232.27	2,479.29

same transaction_id

STRATEGIC DATA CLEANSING

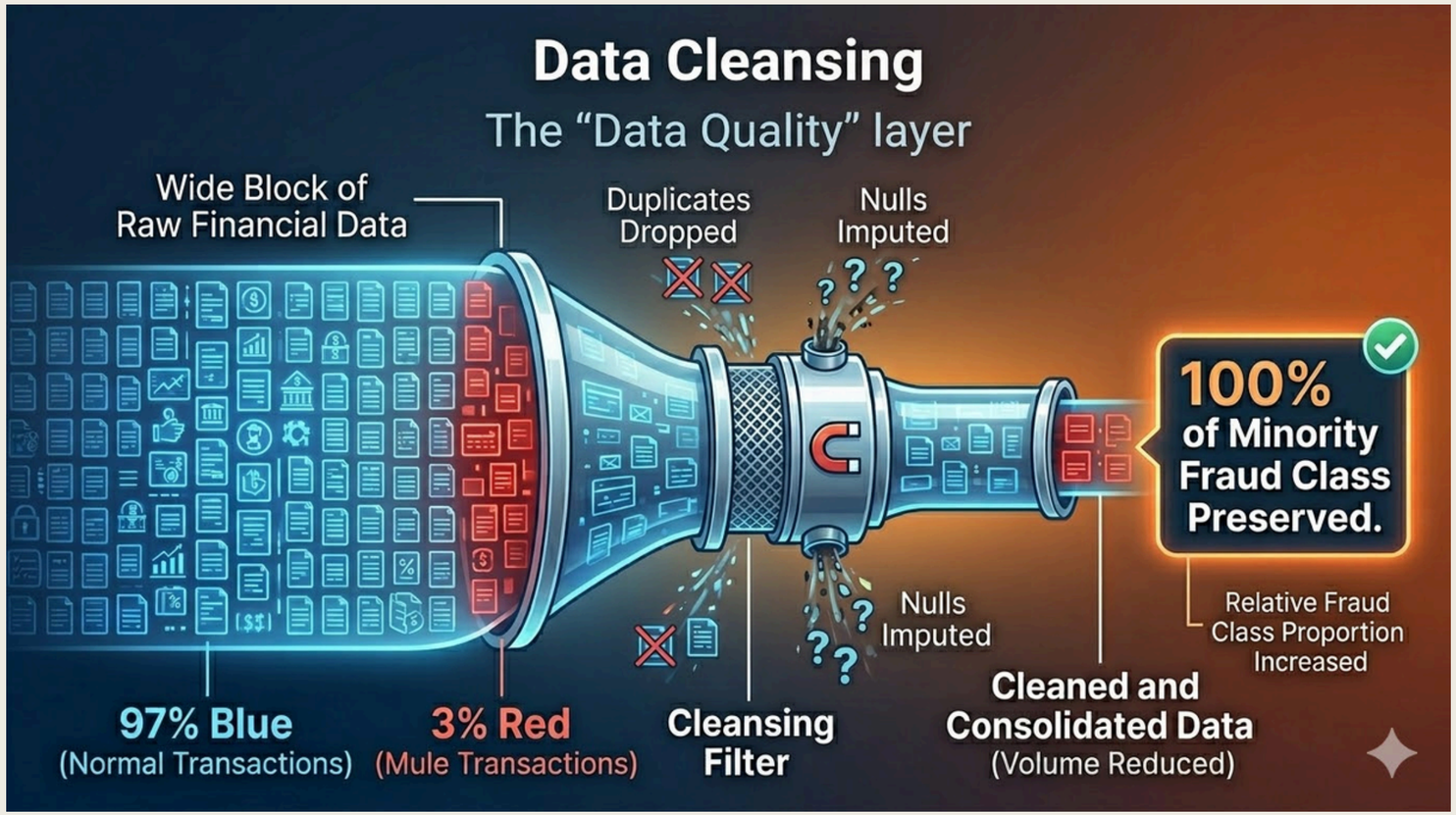
CLEANSING WITHOUT ERASING THE SIGNAL

Fraud accounts represent <3% of the dataset. Careless cleaning destroys the minority class.

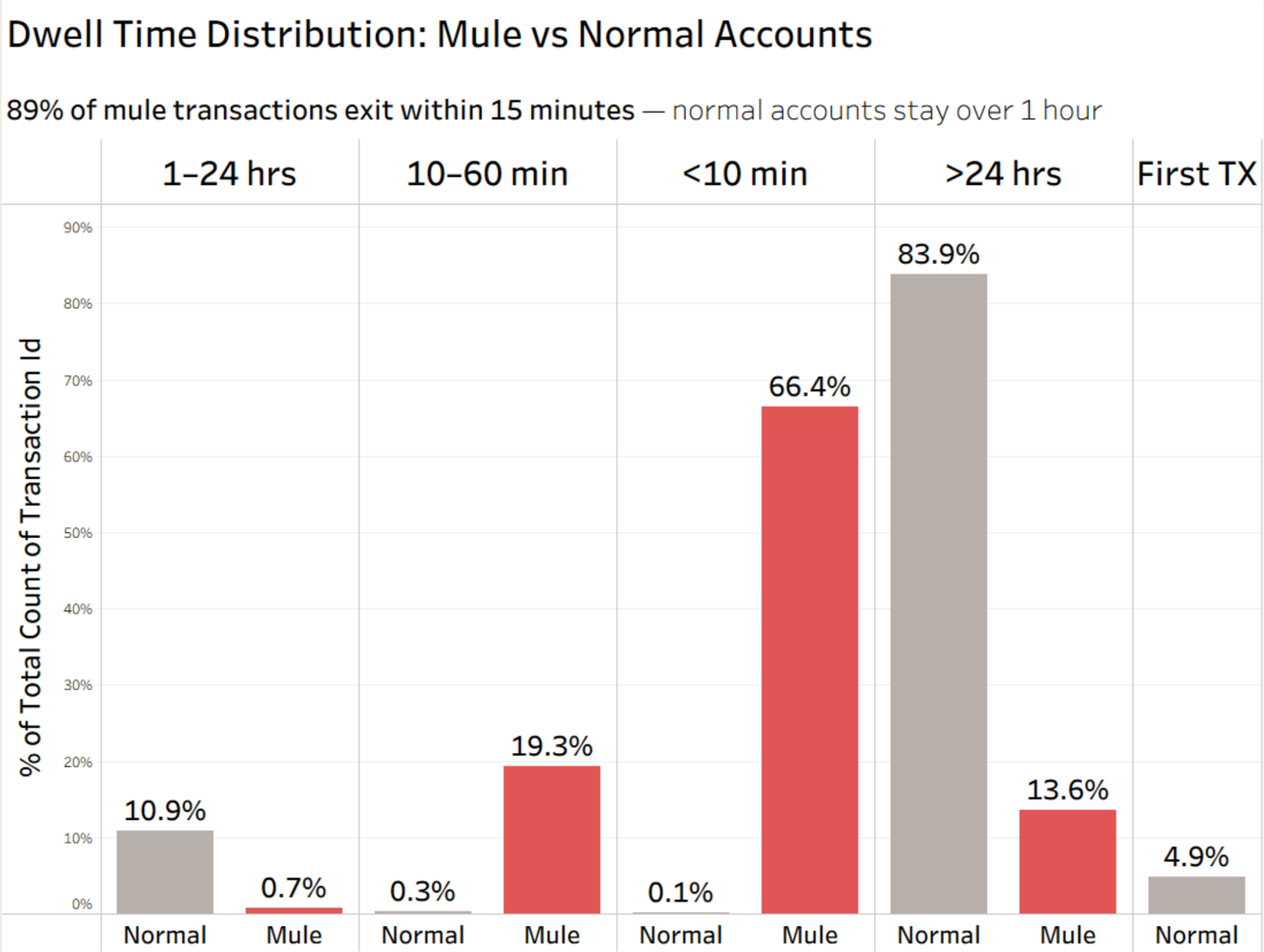
- **Surgical Deduplication:** Remove absolute row-level duplicates to prevent skewed financial volume, but keep identical amounts sent to different receivers.

- **Targeted Imputation:** Do not drop rows with Null device IDs. Impute with "Unknown_Legacy" to preserve the critical financial flow and rolling balances.

- **Value Correction:** Flag negative transaction amounts as human/system data-entry errors and convert to absolute values rather than deleting the record.



DWELL TIME DISTRIBUTION

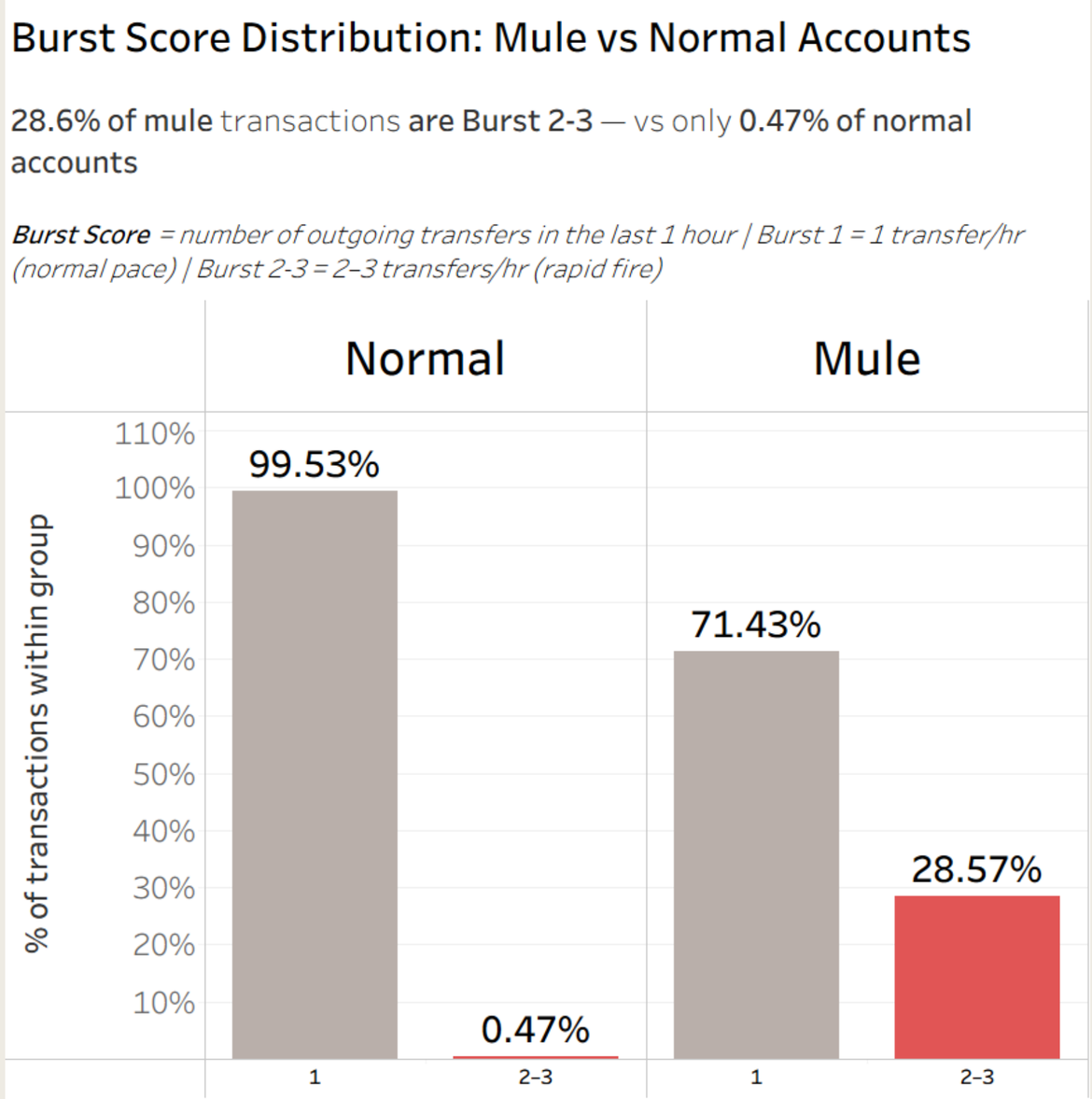


กราฟนี้แสดงสัดส่วนธุรกรรมในแต่ละช่วง DWELL TIME ระหว่างบัญชีม้า (แดง) และบัญชีปกติ (เทา)

พบว่า 39.9% ของธุรกรรมม้าออกภายใน 5 นาที
และอีก 48.4% ออกภายใน 5-15 นาที
รวม 88.3% ออกภายใน 15 นาที

ในขณะที่บัญชีปกติ 94.7% ค้างเงินไว้นานกว่า 1 ชั่วโมง
ยืนยันพฤติกรรม "รับเงินเข้าแล้วโอนออกทันที" (PASS-THROUGH)
และผ่านเกณฑ์ KPI MULE DWELL RATE ≥ 90%

BURST SCORE DISTRIBUTION: MULE VS NORMAL



กราฟนี้เปรียบเทียบการกระจายตัวของธุรกรรมตาม BURST SCORE ระหว่างบัญชีม้า (MULE) และบัญชีปกติ (NORMAL)

พบว่า 28.6% ของธุรกรรมม้าอยู่ในกลุ่ม BURST 2-3 เทียบกับบัญชีปกติที่มีเพียง 0.47%

ยืนยันว่า BURST SCORE เป็นตัวแยกแยะบัญชีม้าออกจากบัญชีปกติได้อย่างชัดเจน — บัญชีม้าโอนถี่ผิดปกติในช่วงเวลาสั้น ขณะที่บัญชีปกติแทบไม่มีพฤติกรรมนี้เลย

BURST SCORE × AMOUNT Z-SCORE HEATMAP

Mule Rate by Burst Score × Amount Z-Score

Burst 2-3 drives 33.6% mule rate — amount size is not the signal

Burst Score = *number of outgoing transfers in the last 1 hour* | Z-Score = *how unusual the transfer amount is vs sender's history*

	Burst Bucket	
Z-Score Bucket	1	2–3
Z 1-2	0.2% (n=2,917)	0.0% (n=12)
Z < 1	0.5% (n=16,127)	33.6% (n=119)
Z > 2	1.6% (n=822)	0.0% (n=3)

กราฟนี้แสดง MULE RATE (%) จากการจัดกลุ่มธุรกรรมตาม BURST SCORE (ความถี่โอนต่อชั่วโมง) และ AMOUNT Z-SCORE (ความผิดปกติของยอดโอน)

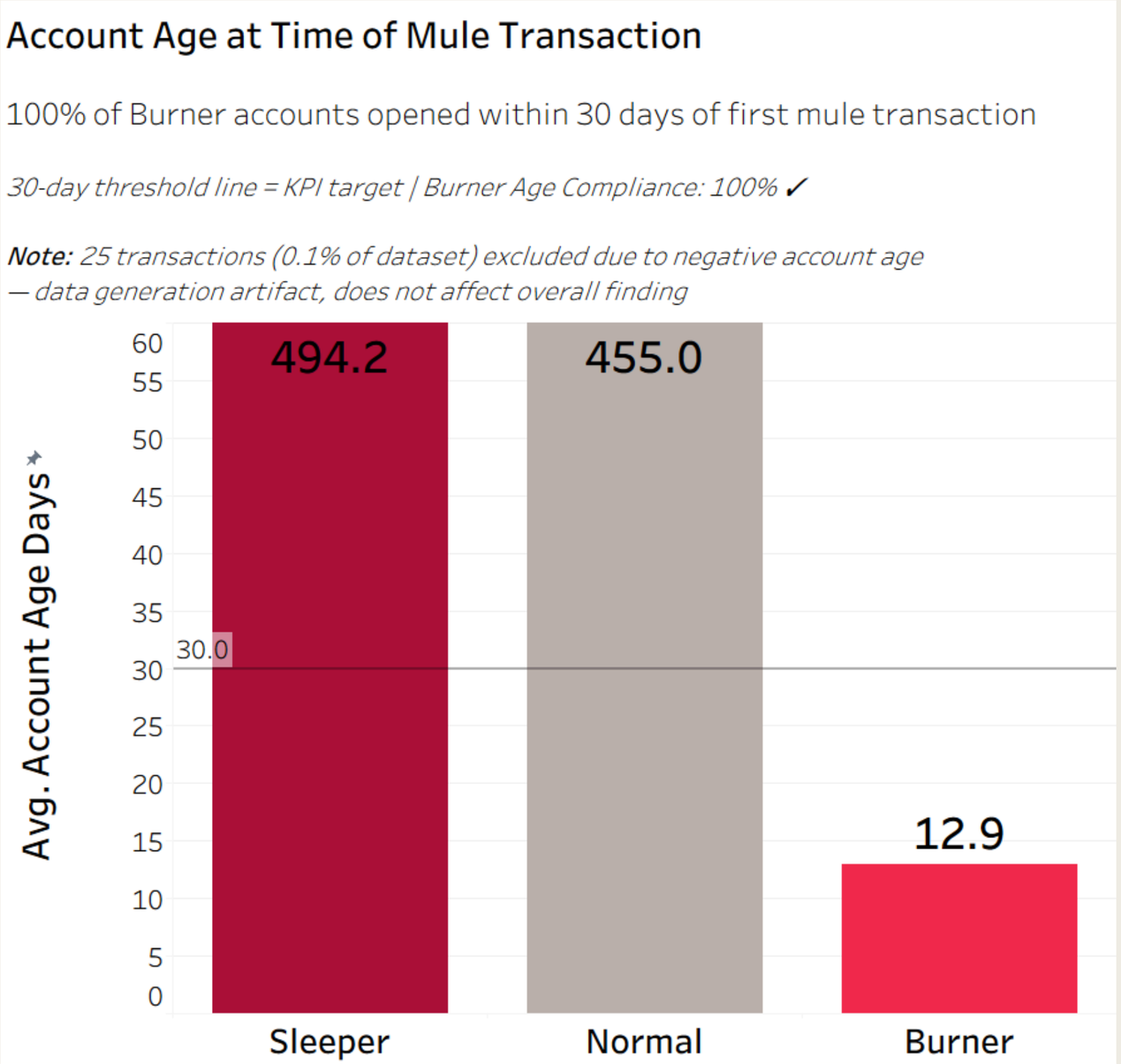
พบว่ากลุ่ม BURST 2-3 ร่วมกับ Z-SCORE ปกติ (< 1) มี MULE RATE สูงถึง 41.7% — สูงกว่า BASELINE ถึง 70 เท่า

ยืนยันว่าบัญชีม้าโอนเงินถี่ในยอดที่ดูปกติ เพื่อหลีกเลี่ยงการตรวจจับด้วยยอดผิดปกติ BURST SCORE คือสัญญาณหลัก — ไม่ใช่ขนาดยอดโอน

ธุรกรรมที่ "ผิดปกติ" ในบริบทนี้ไม่ใช่ยอดโอนสูง
แต่คือการโอนถี่ในยอดปกติ ไปยังผู้รับที่ไม่เคยมีประวัติ
ภายในเวลาไม่กี่นาที

BURNER AGE COMPLIANCE — KPI VERIFICATION

บัญชี BURNER มีอายุเฉลี่ยเพียง 12.9 วัน — ต่ำกว่าเกณฑ์ 30 วันอย่างมีนัยสำคัญ



กราฟนี้แสดงอายุเฉลี่ยของบัญชี (Account Age) ณ วันที่เกิดธุรกรรมม้า จำแนกตามประเภทบัญชี (Burner / Sleeper / Normal)

Burner: อายุเฉลี่ย 12.9 วัน — เปิดบัญชีใหม่เพื่อฟอกเงินโดยเฉพาะ
Sleeper: อายุเฉลี่ย 494.2 วัน — บัญชีเก่าที่ถูก recruit เข้าสู่วงจร
Normal: อายุเฉลี่ย 455 วัน — พฤติกรรมบัญชีปกติ

เส้น 30 วัน คือเกณฑ์ KPI ที่ตั้งไว้
Burner ทุกบัญชีอยู่ต่ำกว่าเส้นนี้ — ยืนยัน KPI Burner Age Compliance 100% ✓

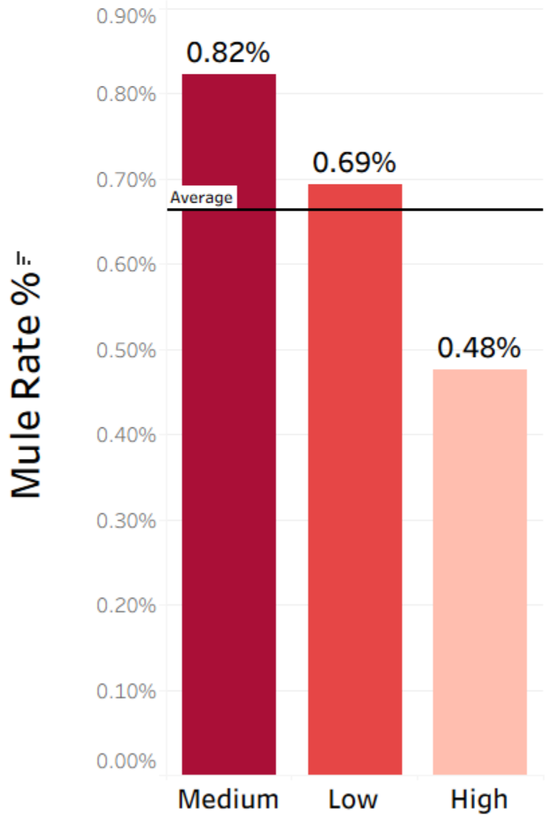
ข้อสังเกต: พบ 25 ธุรกรรม (0.1%) ที่มี Account Age ติดลบ
— เกิดจาก Data Generation Artifact และถูก Exclude ออกจากการวิเคราะห์

WHO IS A MULE? — Risk Profile of Flagged Accounts

Mule Rate by Risk Segment

Medium-risk accounts have highest mule concentration — not High-risk as expected

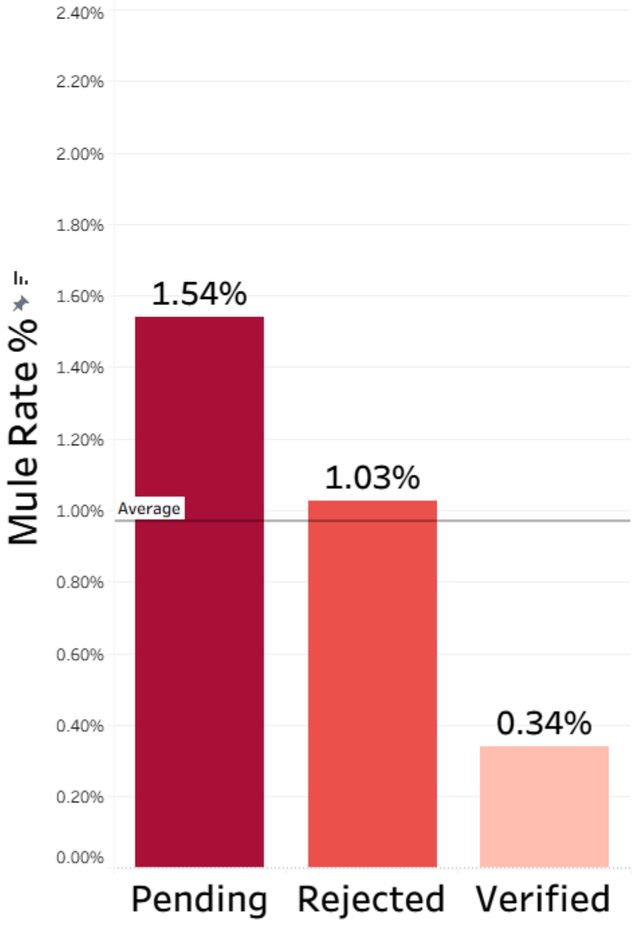
Note: High-risk accounts may be already flagged/blocked by KYC — mules exploit medium-risk blind spots



Mule Rate by KYC Status

Pending KYC = 4.5x mule rate vs Verified — Rejected accounts transacting at all is itself a red flag

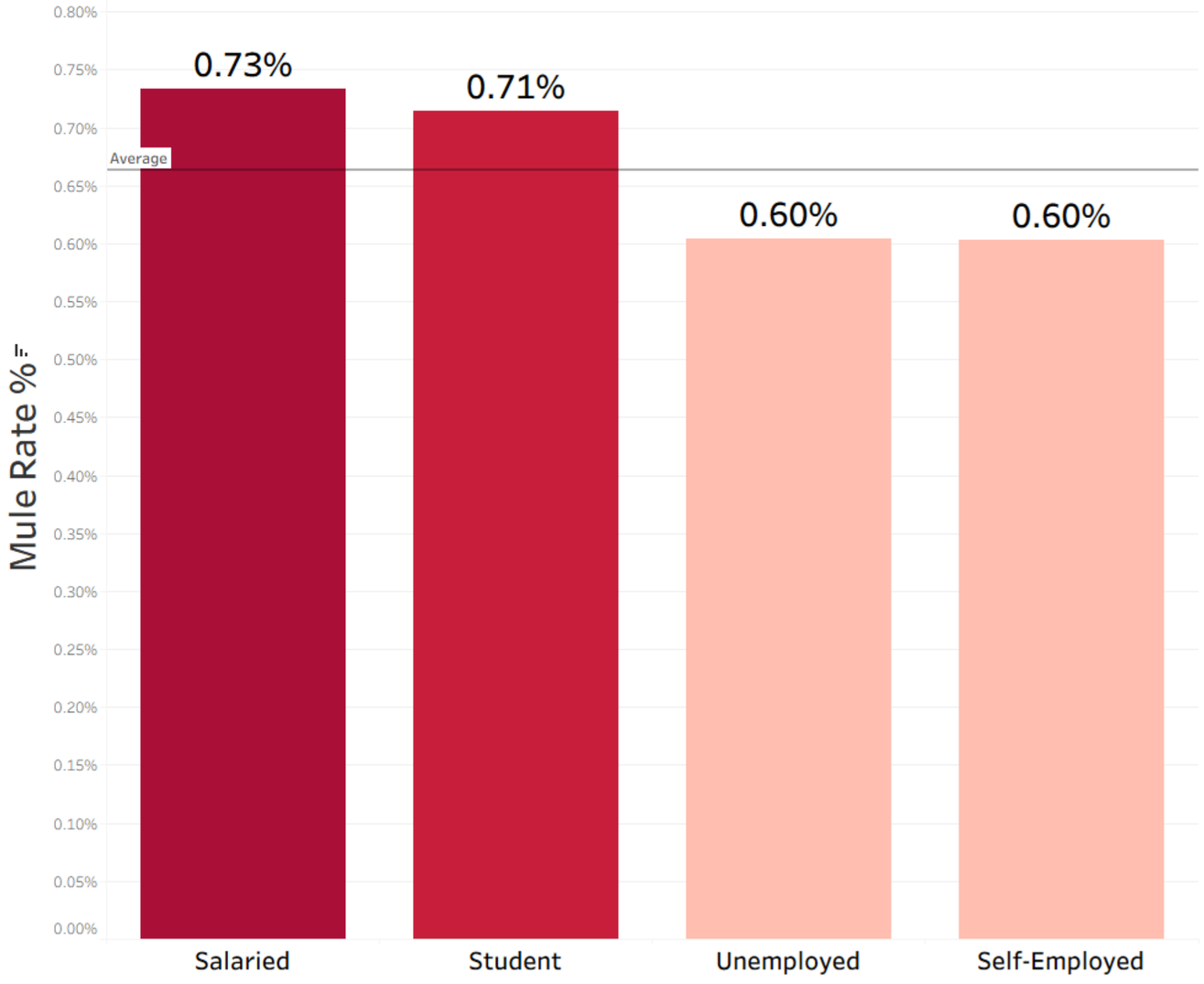
KYC Status *= verification level of the account holder at time of transaction*



Mule Rate by Employment Status

Salaried and Student accounts show highest mule concentration

Salaried accounts may reflect recruitment targeting stable-income individuals for credibility



WHO IS A MULE? — KEY FINDINGS

- **RISK SEGMENT**

กลุ่ม MEDIUM-RISK มี MULE RATE สูงสุดที่ 0.82% — สูงกว่า HIGH-RISK ที่คาดไว้ สะท้อนว่ามิจฉาชีพเลือกเป้าหมายที่ผ่าน KYC แต่ไม่ถูกตรวจสอบเพิ่มเติม

- **KYC STATUS**

บัญชี PENDING (1.54%) และ REJECTED (1.03%) — สูงกว่า VERIFIED ถึง 4.5 เท่า บัญชี REJECTED ที่ยังทำธุรกรรมได้คือสัญญาณอันตรายในตัวเอง

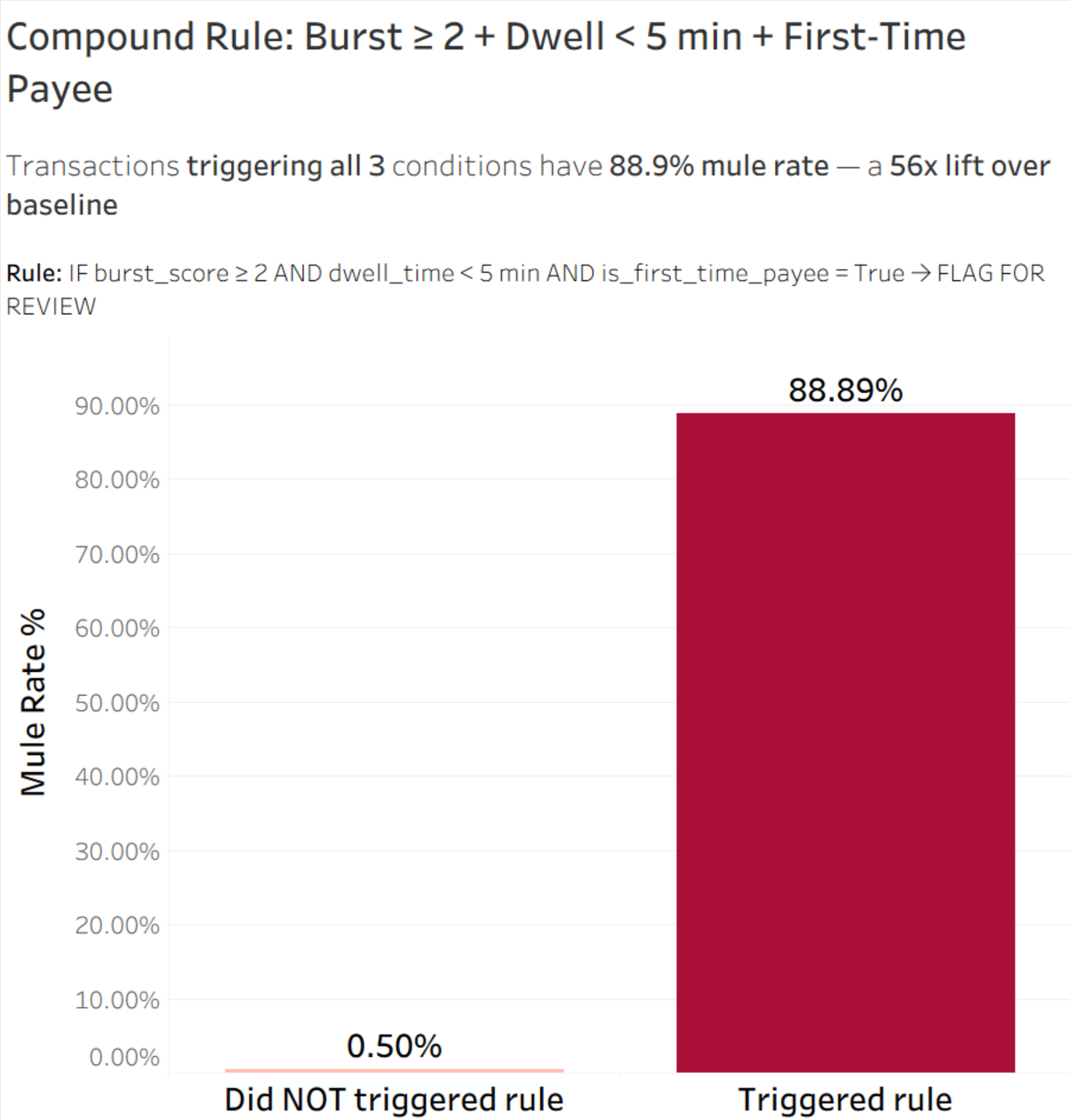
- **EMPLOYMENT**

บัญชี SALARIED (0.73%) และ STUDENT (0.71%) มี MULE RATE สูงสุด — กลุ่มที่มีรายได้มั่นคงและน่าเชื่อถือคือเป้าหมายหลักของการ RECRUIT บัญชีม้า

โปรไฟล์ความเสี่ยงสูงสุด:

PENDING KYC + MEDIUM RISK + SALARIED/STUDENT

COMPOUND RULE: THE DEPLOYABLE DETECTION RULE



กราฟนี้แสดงผลของการรวม 3 สัญญาณเข้าด้วยกัน:
BURST SCORE ≥ 2 + DWELL TIME < 5 นาที + FIRST-TIME PAYEE

พบว่าธุรกรรมที่ TRIGGER ครบทั้ง 3 เงื่อนไข มี MULE RATE สูงถึง 88.89% — สูงกว่า BASELINE (0.89%) ถึง 56 เท่า

หมายความว่าเกือบ 9 ใน 10 ธุรกรรมที่ผ่านเกณฑ์นี้เป็นบัญชีม้า RULE นี้สามารถนำไปใช้คัดกรองได้ทันที โดยไม่ต้องรอ ML MODEL

- False Positive cost: only 5 normal transactions flagged per 20,000 — 0.025% of normal volume. Requires human review, not automatic block.

DEPLOYMENT STRATEGY

FROM DETECTION TO PREVENTION — THREE OPERATIONAL TIERS

TIER 1 — AUTO-FLAG FOR REVIEW

HIGH CONFIDENCE | COMPOUND RULE

TRIGGER: BURST_SCORE ≥ 2 AND DWELL_TIME < 5 MIN AND IS_FIRST_TIME_PAYEE = TRUE

ACTION: HOLD TRANSACTION → MANUAL REVIEW ภายใน SLA

PERFORMANCE:

- **PRECISION:** 88.89%
- **FPR:** 0.025%
- **VOLUME:** ~5 REVIEWS ต่อ 20,000 ธุรกรรม

TIER 2 — ENHANCED MONITORING

MEDIUM CONFIDENCE | RISK STACKING

TRIGGER:KYC_STATUS = PENDING AND RISK_SEGMENT = MEDIUM AND ACCOUNT_AGE < 30 DAYS

- **ACTION:** ไม่ BLOCK ธุรกรรม แต่เพิ่ม **MONITORING FREQUENCY** + ลด THRESHOLD ของ TIER 1 สำหรับบัญชีกลุ่มนี้
- **PURPOSE:** ลด FALSE NEGATIVE ในกลุ่มที่ COMPOUND RULE ยังจับไม่ได้ — ครอบคลุม SLEEPER ACCOUNTS ที่ยังไม่ TRIGGER พฤติกรรม PASS-THROUGH

TIER 3 — PRE-ACTION WARNING

PREVENTION | PROTECT THE RECRUITED

TRIGGER:ACCOUNT_AGE < 30 DAYS AND IS_FIRST_TIME_PAYEE = TRUE AND ยอดโอนสูงผิดปกติ

- **ACTION:** IN-APP WARNING ก่อนกดยืนยันโอน → เตือนความเสี่ยงการถูกใช้เป็นบัญชีม้า + ลิงก์รายงานเหตุ
- **PURPOSE:** จับจังหวะก่อน BURNER ทำหน้าที่ PASS-THROUGH จริง — ปกป้องผู้ที่ถูก RECRUIT โดยไม่รู้ตัว

TRADE-OFF SUMMARY

Tier	Friction	Precision	Coverage
Tier 1	High (block)	88.89%	Narrow
Tier 2	None (watch)	Medium	Broad
Tier 3	Low (warn)	Prevention	Pre-event

KPI VERDICT — DID WE MEET OUR TARGETS?

KPI	Target	Actual	Status
Compound Rule Precision	≥ 50%	88.89%	Pass (1.8x target)
Compound Rule FPR	≤ 0.05%	0.03%	Pass
Mule Dwell Rate	≥ 90%	88.30%	Near miss
In/Out Mule Lift	≥ 2.0x	2.8x	Pass
Burst Lift (2–3 vs Normal)	—	59x	Strong signal*
Burner Age Compliance	100%	100%	Pass
Night Activity Lift	≥ 2.0x	N/A	Limitation
API Concentration	≥ 50%	15%	Limitation

*Burst KPI ปรับจาก "% Hop 2 ที่ Burst ≥ 3" เป็น Lift Analysis — ให้สัญญาณที่แยกแยะคมชัดกว่า (28.6% mule vs 0.47% normal)

LIMITATION

WHERE: API CHANNEL SHOWED 15% MULE CONCENTRATION VS ≥50% TARGET — SYNTHETIC DATA LIMITATION, NOT ENOUGH BEHAVIORAL DIFFERENTIATION IN TRANSFER METHOD ASSIGNMENT

WHEN: HOURLY SIGNAL EXISTS BUT NOT INDEPENDENTLY ACTIONABLE — REMOVED FROM ANALYSIS SCOPE AS IT CANNOT FORM A STANDALONE RULE

OUR TEAM

RATTANIN KLIANGMOL 252

PASUWAT THANGKONGNUCH 179

PURIN BOONPETCH 250