Laporan Analisis Penipuan Platform Pembayaran

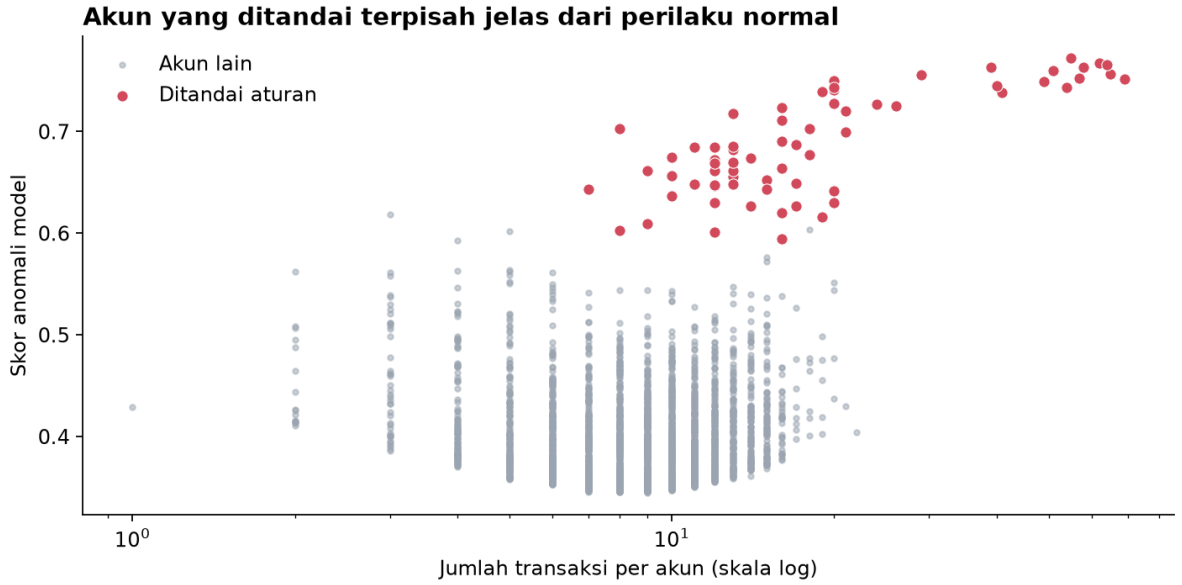
Studi kasus portofolio dengan data sintetis. Periode 2026-09-01 s.d. 2026-10-30.

Catatan keterbukaan

Seluruh data di laporan ini dibuat sendiri untuk meniru ekspor transaksi, log aktivitas, dan catatan tim internal. Tidak ada data klien yang dipakai. Pola penipuan disisipkan lebih dulu dengan kunci jawaban yang disimpan terpisah, lalu aturan dibuat tanpa membuka kunci itu. Karena pola sintetis relatif bersih, angka akurasi di bawah menunjukkan cara kerja metode, bukan janji hasil pada data nyata.

Ringkasan temuan

Dari 28,366 transaksi (3,000 akun, nilai pembayaran Rp4.552.829.616), analisis menandai **67 akun** dengan aturan berbobot. 67 di antaranya benar-benar akun curang, 0 salah tandai, dan 2 akun curang lolos. Presisi 100%, recall 97%. Nilai pembayaran yang melewati akun curang mencapai **Rp1.299.506.169**.



Metodologi

1. Pembersihan. Transaksi dipisah menurut tipe (bayar, refund, ganti sandi); waktu diseragamkan; kolom jawaban tidak ada di data yang dianalisis.

2. Fitur per akun. Jumlah dan nilai transaksi, rasio gagal, kecepatan (transaksi terbanyak dalam 10 menit), jumlah perangkat dan kota, transaksi mepet batas Rp5 juta, rasio refund, jumlah akun per perangkat, dan transaksi setelah ganti sandi.

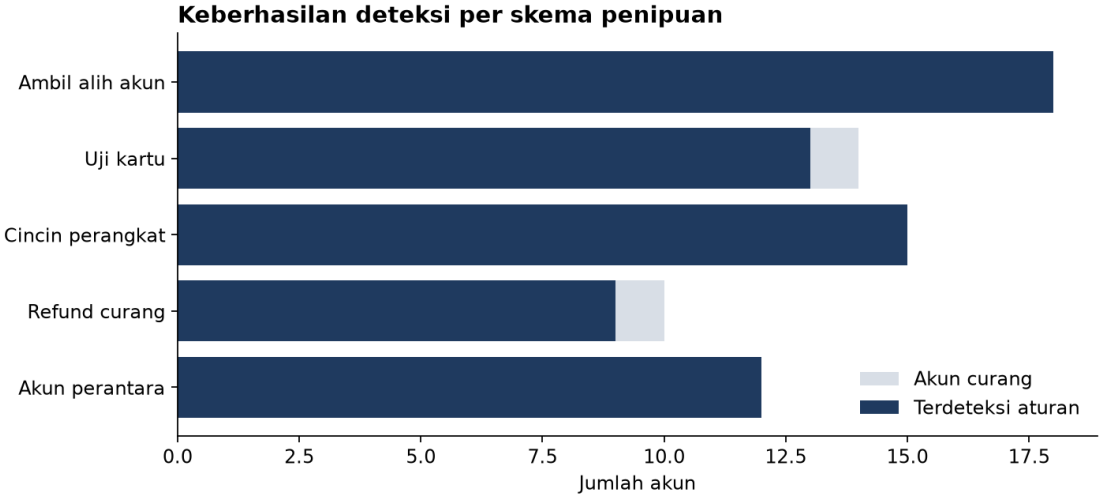
3. Aturan berbobot. Delapan aturan yang bisa dibaca orang (tabel di bawah). Akun dengan skor 3 atau lebih dipantau; skor 6 atau lebih berprioritas tinggi.

4. Model pendamping. Isolation Forest (300 pohon) memberi skor keanehan tanpa label. Dipakai sebagai lapis kedua, bukan penentu tunggal.

5. Evaluasi. Baru di akhir, hasil dibandingkan dengan kunci jawaban.

Aturan deteksi dan seberapa sering terpicu

Kode	Aturan	Bobot	Akun terpicu
R1	Uji kartu: >=8 transaksi dalam 10 menit dan >=50% gagal	4	13
R2	Transaksi berlebih bernilai kecil (>=15 transaksi <= Rp10 ribu)	2	14
R3	Belanja besar setelah ganti sandi (<30 menit)	4	18
R4	Transaksi dari luar negeri oleh akun domestik	3	18
R5	Pola pemecahan: >=5 transaksi Rp4,5-5 juta	4	12
R6	Akun baru (<14 hari) dengan total belanja > Rp20 juta	3	12
R7	Refund berulang: >=5 refund dan rasio >= 40%	4	9
R8	Perangkat dipakai >=10 akun berbeda	4	15



Perbandingan metode

Metode	Ditandai	Benar	Salah tandai	Terlewat	Presisi	Recall
Aturan (skor>=3)	67	67	0	2	100%	97%
Isolation Forest saja	90	69	21	0	77%	100%
Aturan + tinjau tambahan IF	68	68	0	1	100%	99%

Isolation Forest sendirian menangkap semua akun curang tetapi menandai 21 akun biasa. Aturan sendirian lebih bersih tetapi melewatkan 2 akun. Menggabungkan keduanya (model hanya menaikkan akun yang sudah punya sedikit sinyal aturan) memberi hasil terbaik.

Daftar akun yang ditandai (20 teratas)

Akun	Prioritas	Skor	Alasan	Jml trx	Total
U00828	Tinggi	7	Pola pemecahan: >=5 transaksi Rp4,5-5 juta; Akun baru (<14 hari) dengan total belanja > Rp20 juta	29	Rp63.406.256
U01089	Tinggi	7	Pola pemecahan: >=5 transaksi Rp4,5-5 juta; Akun baru (<14 hari) dengan total belanja > Rp20 juta	20	Rp43.725.496
U02447	Tinggi	7	Pola pemecahan: >=5 transaksi Rp4,5-5 juta; Akun baru (<14 hari) dengan total belanja > Rp20 juta	20	Rp48.297.387
U01305	Tinggi	7	Pola pemecahan: >=5 transaksi Rp4,5-5 juta; Akun baru (<14 hari) dengan total belanja > Rp20 juta	20	Rp63.173.553
U00242	Tinggi	7	Pola pemecahan: >=5 transaksi Rp4,5-5 juta; Akun baru (<14 hari) dengan total belanja > Rp20 juta	19	Rp53.331.473
U00257	Tinggi	7	Pola pemecahan: >=5 transaksi Rp4,5-5 juta; Akun baru (<14 hari) dengan total belanja > Rp20 juta	20	Rp68.554.773
U00495	Tinggi	7	Pola pemecahan: >=5 transaksi Rp4,5-5 juta; Akun baru (<14 hari) dengan total belanja > Rp20 juta	24	Rp49.074.825
U01695	Tinggi	7	Pola pemecahan: >=5 transaksi Rp4,5-5 juta; Akun baru (<14 hari) dengan total belanja > Rp20 juta	26	Rp72.922.716
U02573	Tinggi	7	Pola pemecahan: >=5 transaksi Rp4,5-5 juta; Akun baru (<14 hari) dengan total belanja > Rp20 juta	16	Rp52.996.965
U00470	Tinggi	7	Pola pemecahan: >=5 transaksi Rp4,5-5 juta; Akun baru (<14 hari) dengan total belanja > Rp20 juta	21	Rp55.320.144
U02202	Tinggi	7	Pola pemecahan: >=5 transaksi Rp4,5-5 juta; Akun baru (<14 hari) dengan total belanja > Rp20 juta	13	Rp43.359.850
U00105	Tinggi	7	Pola pemecahan: >=5 transaksi Rp4,5-5 juta; Akun baru (<14 hari) dengan total belanja > Rp20 juta	16	Rp38.387.988
U02023	Tinggi	7	Belanja besar setelah ganti sandi (<30 menit); Transaksi dari luar negeri oleh akun domestik	17	Rp21.637.547
U02316	Tinggi	7	Belanja besar setelah ganti sandi (<30 menit); Transaksi dari luar negeri oleh akun domestik	12	Rp26.234.009
U00623	Tinggi	7	Belanja besar setelah ganti sandi (<30 menit); Transaksi dari luar negeri oleh akun domestik	16	Rp26.415.378
U01995	Tinggi	7	Belanja besar setelah ganti sandi (<30 menit); Transaksi dari luar negeri oleh akun domestik	13	Rp14.597.534
U01680	Tinggi	7	Belanja besar setelah ganti sandi (<30 menit); Transaksi dari luar negeri oleh akun domestik	9	Rp24.100.383
U00335	Tinggi	7	Belanja besar setelah ganti sandi (<30 menit); Transaksi dari luar negeri oleh akun domestik	10	Rp25.929.751
U00925	Tinggi	7	Belanja besar setelah ganti sandi (<30 menit); Transaksi dari luar negeri oleh akun domestik	15	Rp16.165.966
U01228	Tinggi	7	Belanja besar setelah ganti sandi (<30 menit); Transaksi dari luar negeri oleh akun domestik	17	Rp31.476.195

Daftar lengkap 68 akun ada di akun_mencurigakan.csv.

Rekomendasi

Blokir perangkat bersama. Satu perangkat yang dipakai 10 akun atau lebih hampir pasti cincin penipuan; blokir otomatis dan tinjau semua akunnya (R8). Catatan tim risiko sudah menyebut perangkat ini tetapi belum diblokir.

Pasang batas kecepatan. Tahan transaksi ke-8 dalam 10 menit bila rasio gagal tinggi dan minta verifikasi tambahan (R1, R2).

Verifikasi ulang setelah ganti sandi. Beri jeda atau OTP tambahan untuk transaksi besar dalam 30 menit setelah ganti sandi, apalagi dari luar negeri (R3, R4).

Pantau nominal mepet batas. Pemecahan di Rp4,5 sampai 5 juta oleh akun baru adalah tanda akun perantara; tambahkan peringatan pada akun di bawah 14 hari (R5, R6).

Batasi refund berulang. Tandai akun yang rasio refund-nya di atas 40% setelah 5 refund (R7).

Eskalasi laporan pelanggan. Delapan laporan CS dalam data tidak dieskalasi; hubungkan laporan "transaksi tidak dikenal" langsung ke antrean tinjauan risiko.

Kurangi salah tandai. Beri daftar putih untuk pelanggan korporat lama yang nominalnya besar, seperti kasus yang dicatat tim risiko.

Keterbatasan

Data sintetis dengan lima pola yang bersih; data nyata lebih berisik dan pelaku menyesuaikan diri. Ambang aturan harus dikalibrasi ulang pada data klien, dan angka presisi serta recall perlu diukur lagi dengan label hasil investigasi nyata. Model dilatih tanpa label sehingga tidak bisa menjelaskan sendiri alasan penandaan; aturan yang menjadi penjelas.