ScotiaShield: Protecting Your Assets with AI-Powered Anomaly Detection

Team 19

THE TEAM

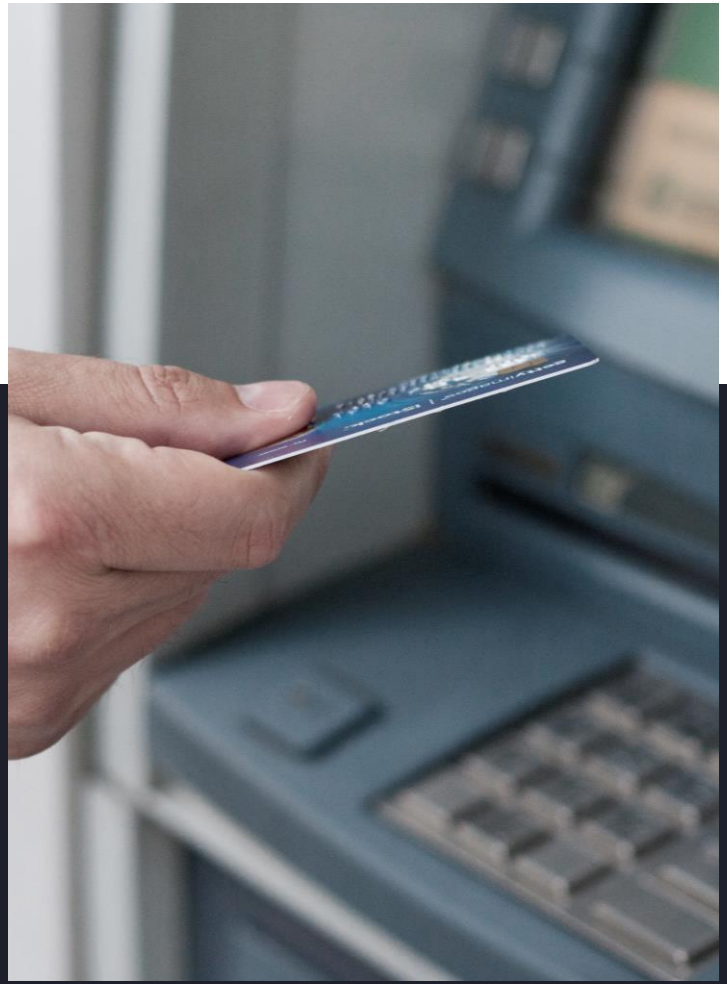
Nikaran K M

Kevin Abdo

Ruiyun (Tracy) Chao

Olivia Woodman

TABLE OF CONTENTS



01

PROBLEM & APPROACH

THE NEED FOR MONEY LAUNDERING DETECTION

Protecting Scotiabank & Customers

Safeguard assets, reputation, and customer trust.

Regulatory Compliance

Stringent regulations (FINTRAC, international bodies).

Moving Targets

Detecting evolving tactics threatening Scotiabank.

Our Solution for Scotiabank: A sophisticated Anti-Money Laundering system designed for comprehensive anomaly detection, tailored to the needs of a major financial institution.

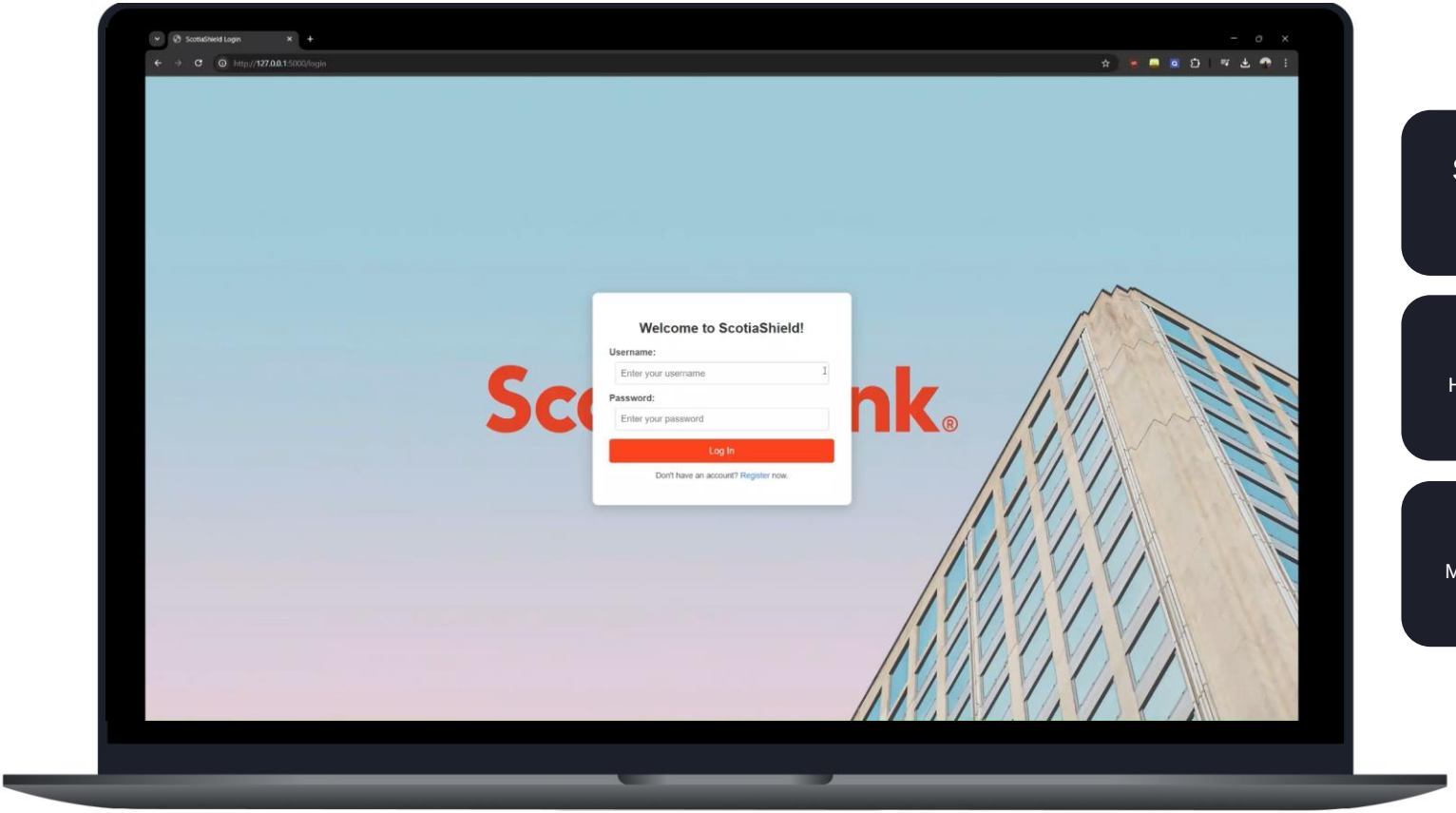
ANALYTICAL CHALLENGES

WHAT ARE THE KEY MOTIVATIONS AND CHALLENGES?

THE COST OF FALSE POSITIVES	UNLABELED DATA	THE INTERPRETABILITY TRADE-OFF
Labour & time to review flagged customers	A lack of labelled datasets necessitates unsupervised learning	Interpretability is beneficial to investigators, regulators, and customer experience
Negative customer experience if falsely identified as fraudulent	Algorithmic performance is not easily measured	The most interpretable methods are the most inaccurate

We are closing the loop between human insight and AI in money laundering detection

USER INTERFACE: Employee Login

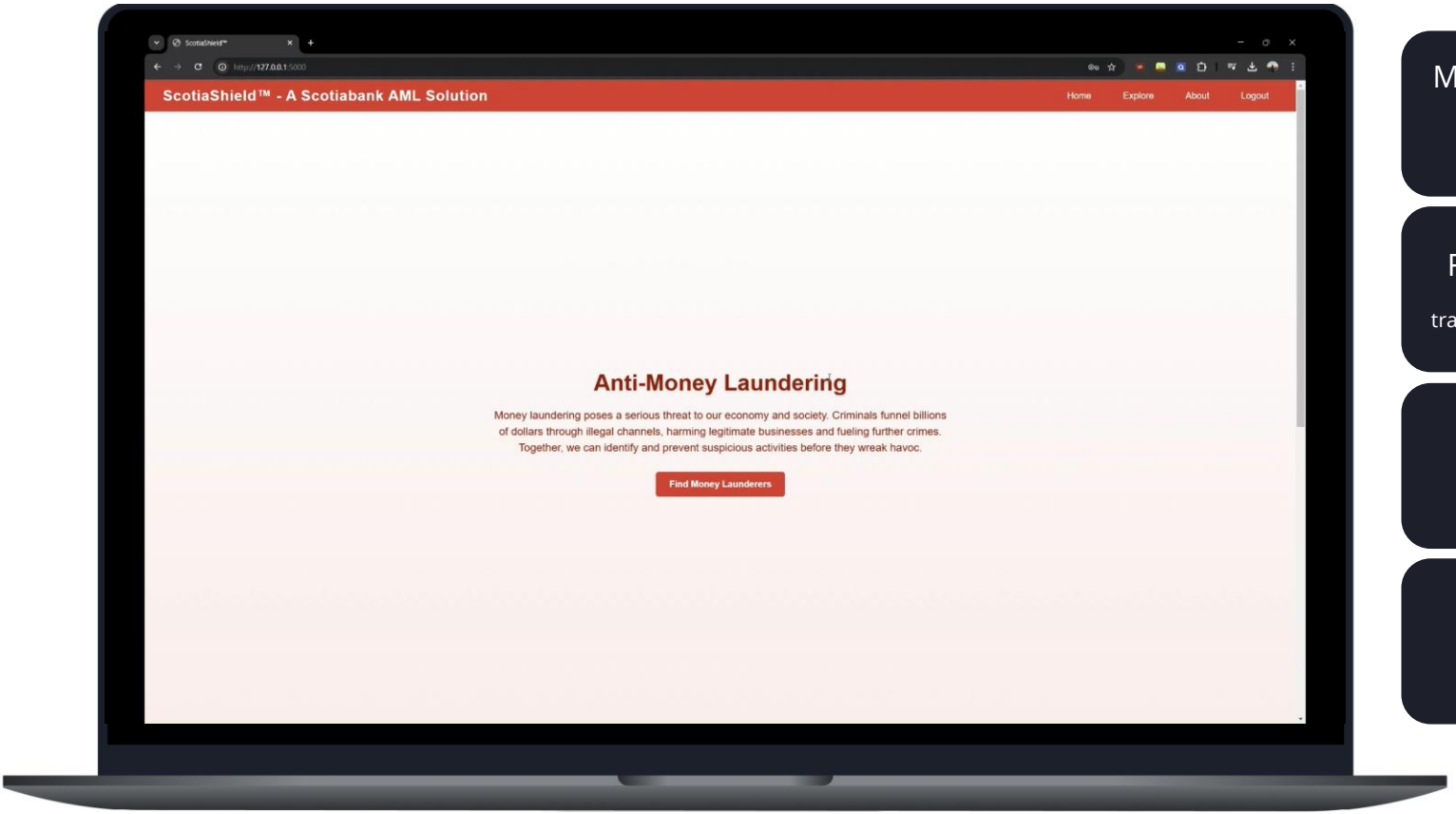


Streamlined Web App
Developed using Python Flask, HTML, CSS, SQLite

Secure Access
Hashing, role-based permissions, session management

Easy Onboarding
Minimal steps, guided registration, automated welcome

USER INTERFACE: Alert Dashboard



ML-Selected Customers

View thousands of machine learning identified suspicious customer transactions

Flagging Transactions

Human agents can flag certain transactions to review them further

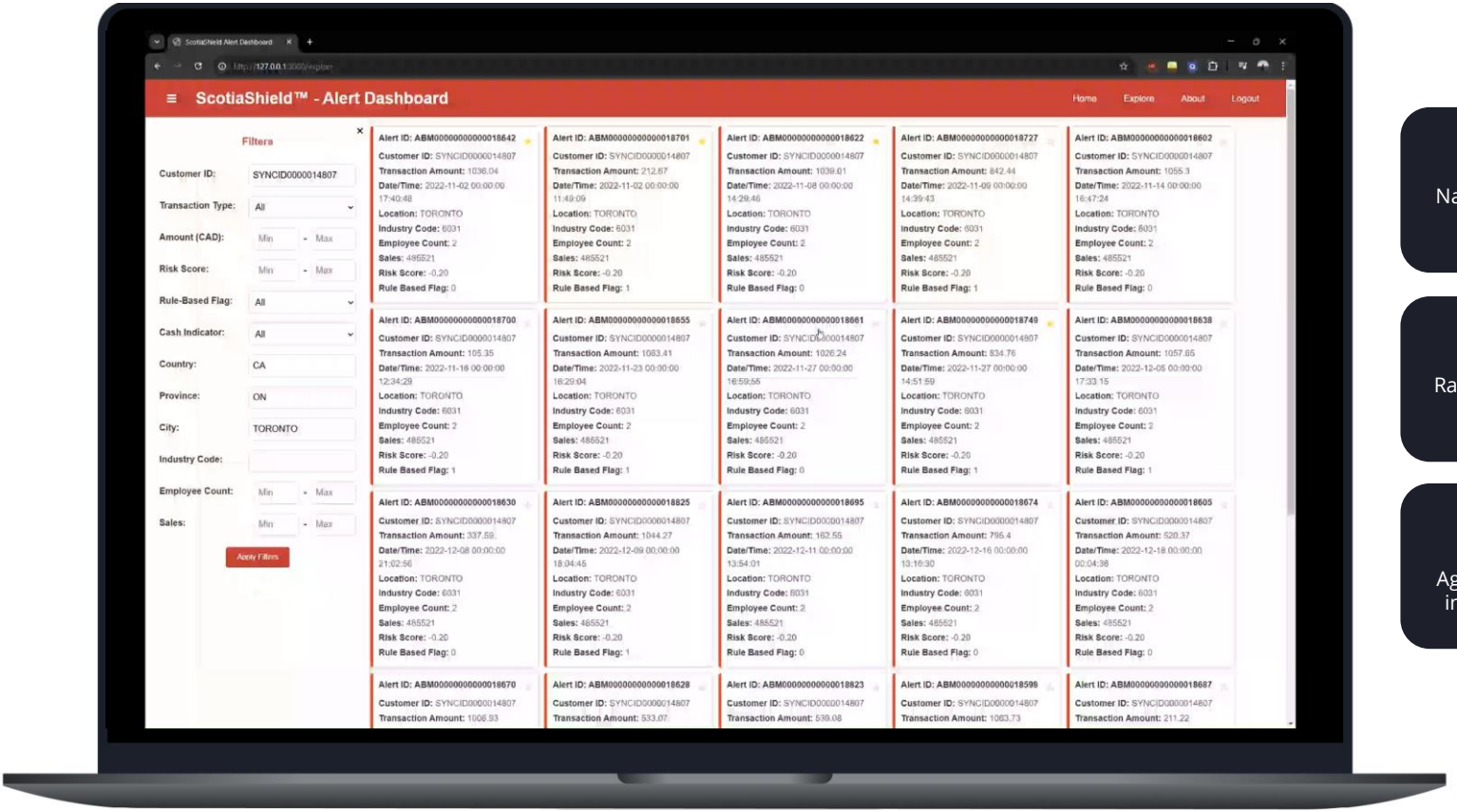
Easy Filtering

View transactions that fulfill specified criteria

Rule-based flags

Further classify suspicious transactions using risk factors

USER INTERFACE: Save Session & Exit



Easy Navigation

Navigation bar allows for easy and intuitive website use

About Section

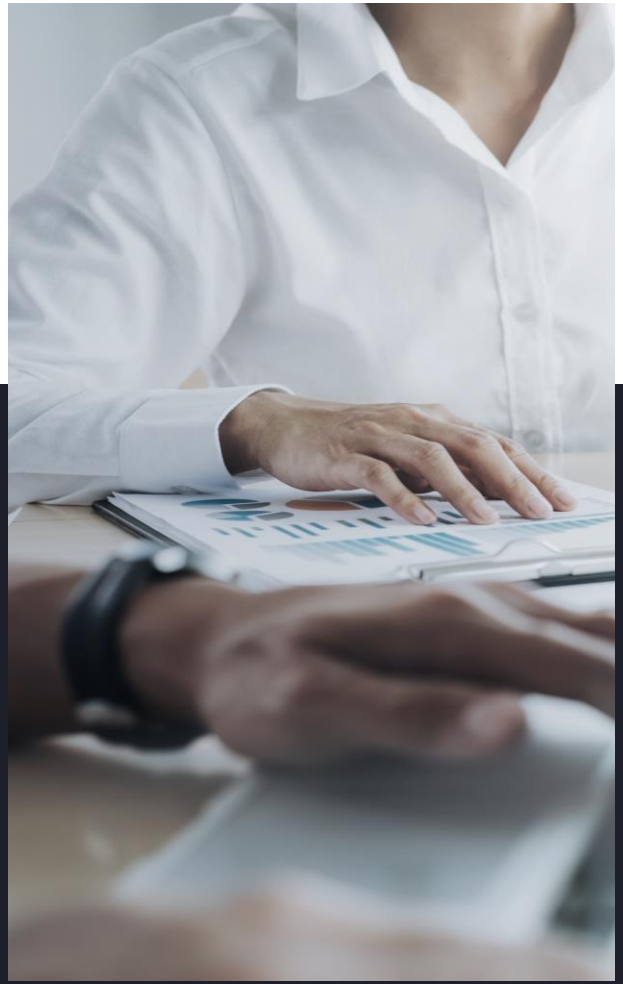
Raise awareness of the institutions involved and their importance

Logout and Save Session

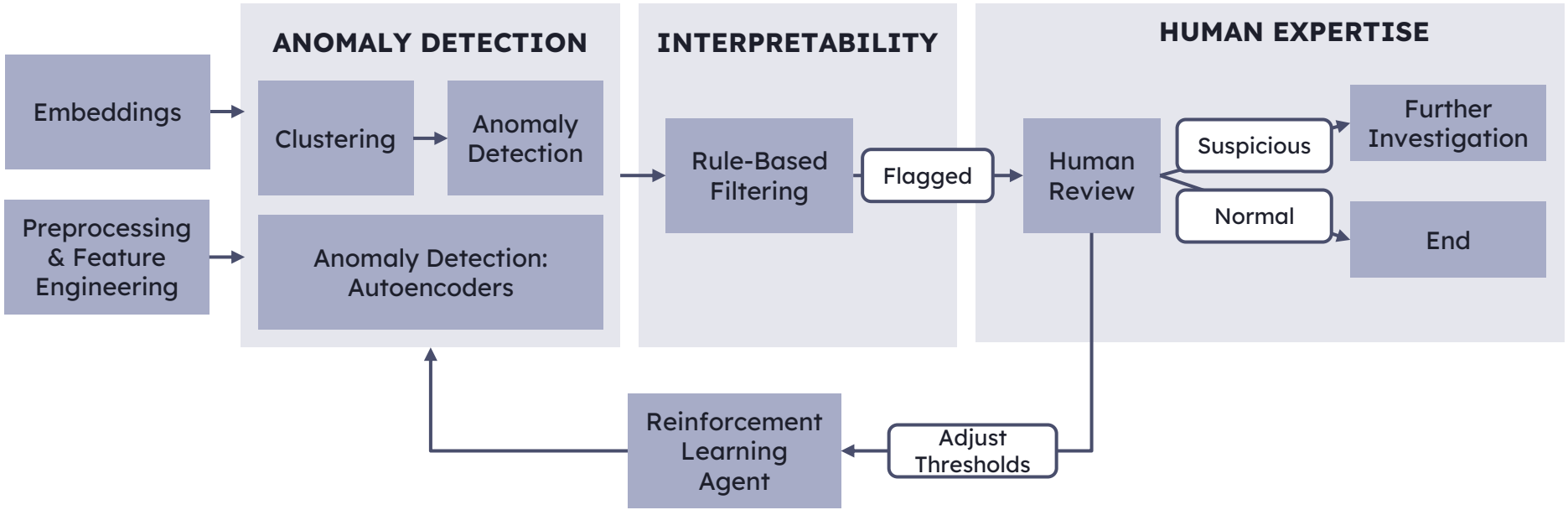
Agents can come back and further investigate the transactions they have flagged

02

METHODOLOGY



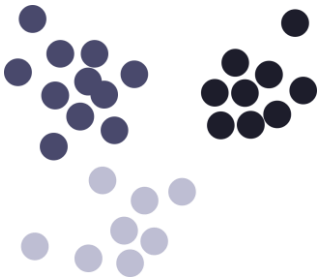
SOLUTION OVERVIEW



AI METHODS

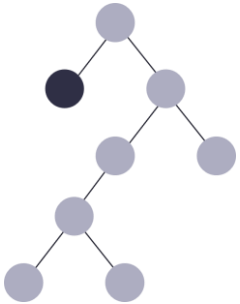
ANOMALY DETECTION

CLUSTERING & K-Means



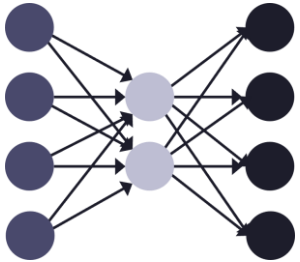
By clustering similar customers, we can find outliers that from any other points, or use clusters for segmentation

ISOLATION FORESTS



A binary tree method that can be applied to each customer to find anomalies. The level of “contamination” is set by the user.

AUTO-ENCODERS

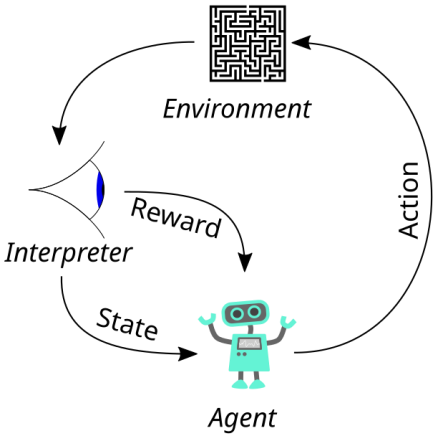


A neural network that encodes then decodes the input. Anomalies are points that are difficult to reconstruct.

Reinforcement Learning

RL Overview

- RL agents learn to **assign risk scores** based on historical data and predefined rules.
- The goal is to maximize the detection of fraudulent transactions while **minimizing false positives**.
- Agents **continuously update their policies** based on feedback (rewards) from the environment.



RL Rules – What makes a customer high risk?*

- **Time-Based**: Late-night/weekend transactions
- **Frequency**: High-frequency or sudden changes
- **Geography**: Non-Canada/USA or country mismatch
- **Amount**: Large transactions
- **Industry**: High industry risk scores (> 0.7)
- **Statistical Features**: Unusual average, maximum, or standard deviation of transaction amounts

* For full list of rules, see Appendix

ENGINEERED FEATURES

Transaction Aggregates

- Aggregated for each transaction type
- Separate counts for credit and debit transactions
- 30-day and 7-day rolling averages and sums

Time-Based

- Days since account establishment
- Days since the last transaction
- Log-transformed active days for each transaction method

Risk Scores

- Integrated risk scores based on KYC and industry codes
- Incorporating customer data (e.g., employee count, sales volume)

Ratios

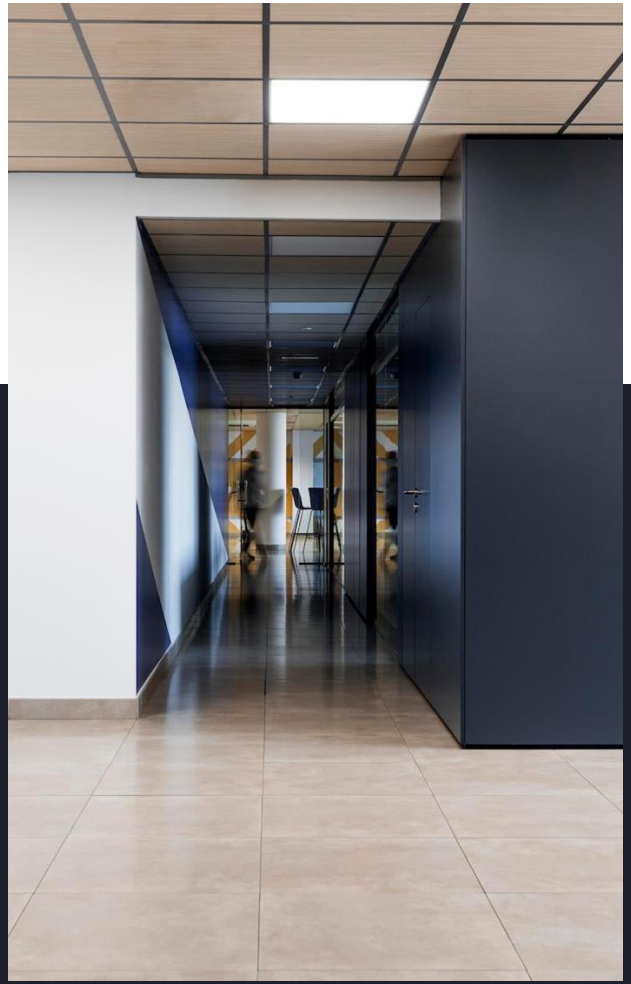
- For all payment channels
- Transaction count to active days, max to average transaction amounts

Atypical Activity

- Identifying unusually high or low transaction amounts
- Highlighting accounts with minimal transaction behavior

ANOMALY DETECTION - VARIABLE SELECTION

Iteration 1 Logical/Mathematical Approach	Based on transaction counts, amounts, timing, ratios, and active days.
Iteration 2 Money Laundering Theory	Focused on placement, layering, integration, and credit/debit ratios.
Iteration 3 Data-Driven/ Unconventional Insights	Examines channel profiles, intensity versus duration, ratio-based metrics, extreme values, and low activity indicators.



03

RESULTS

You can enter a subtitle here if you need it

DETECTED ANOMALIES TO FEED INTO RL

2484

Companies identified

Algorithm	Common Anomalies	Iteration 1 - Unique Anomalies	Iteration 2 - Unique Anomalies	Iteration 3 - Unique Anomalies
Auto-encoder	160	129	89	280
Birch	269	285	175	794
K-means	270	251	242	762

Comparison	Embeddings As Inputs To Cluster	Regular Cluster Models
Common Anomalies	342	342
Unique Anomalies	896	1246

ANOMALIES BY INDUSTRY

TOP 5 INDUSTRIES BY SIZE

1. Other - 285
2. Holding Companies - 140
3. Management Consulting Services - 118
4. General Freight Trucking Industry - 93
5. Offices of Lawyers and Notaries – 78

TOP 5 INDUSTRIES BY %

1. Drugs, Wholesale – 45.4%
2. Sheet Metal and Built-Up Roofing – 41.7%
3. Other Truck Transport Industries – 39.1%
4. Jewellery Stores – 36.8%
5. Disinfecting and Exterminating Services – 31.2%

Chi-squared Test Results

Purpose: Test the association between anomaly status and industry codes.

Findings: Statistically significant association between anomaly status and industry codes ($p < 0.05$).

Interpretation: Anomalies are not evenly distributed across different industry sectors; there is a potential relationship between industry and the likelihood of anomalous behavior.

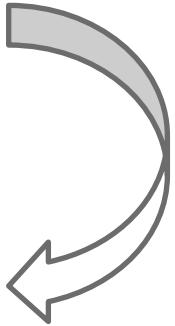
RL Result

Using the subset for **200** / 2484 customers detected by clustering method

Risk Flags

SYNCID0000008332	297
SYNCID0000004200	198
SYNCID0000009041	134
SYNCID0000003996	87
SYNCID0000000721	84
SYNCID0000008301	63
SYNCID0000014643	63
SYNCID0000008903	52
SYNCID0000014811	48
SYNCID0000011844	48
SYNCID0000008897	41
SYNCID0000014637	15
SYNCID0000007445	13
…	
SYNCID0000002597	1
SYNCID0000009755	1
etc	

Number of Risk Flags	Count
297	1
198	1
134	1
87	1
84	1
…	…
1	23



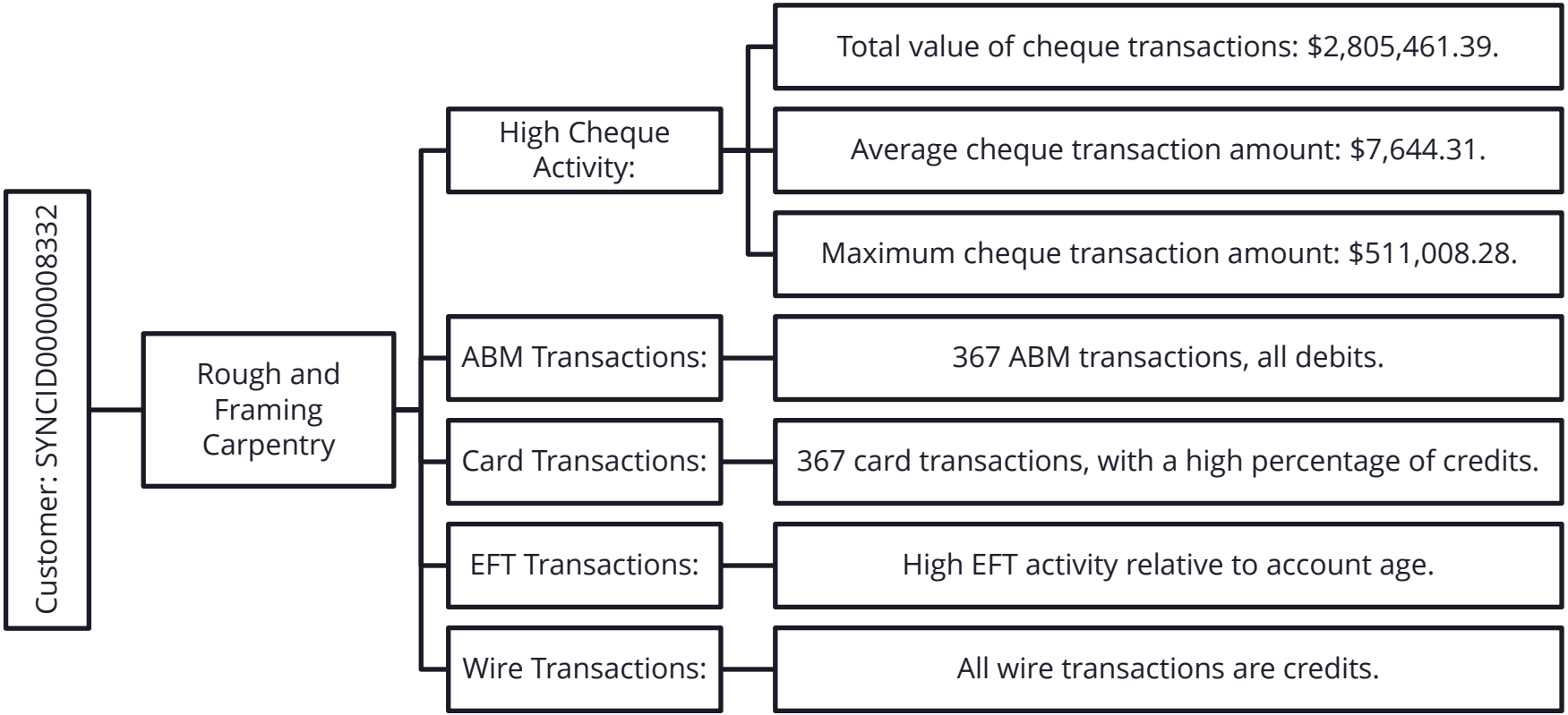
False Positive Rate

46 / 200 = 77%

estimated ML rate

15.3% * 8.5% = 1.3%

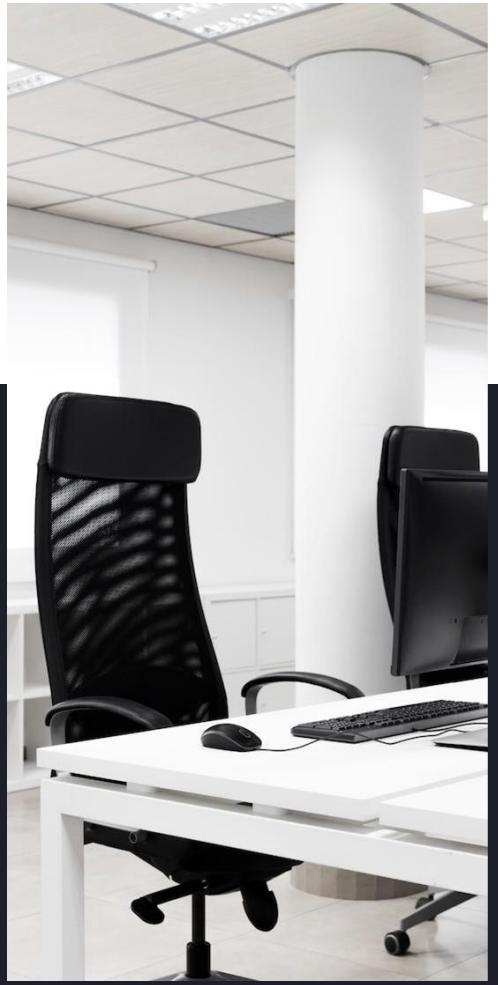
SPOTLIGHT: LIKELY FRAUD



04

CONCLUSIONS

You can enter a subtitle here if you need it



CONCLUSIONS

Diverse Anomaly Detection

K-Means, Birch, and Autoencoder algorithms to find unusual activities.

Catch All True Positives

Focus on finding all real money laundering cases.

Reduce False Positive

Reinforcement Learning helps us avoid wasting time on false alarms.

Unique Findings

Our method finds many unique cases of suspicious behavior.

Industry Matters

The type of industry can affect the chance of money laundering.

Complete Solution

A thorough and effective way to find and stop money laundering.

NEXT STEPS

Key Features of the Website

- **Case Management:** User-friendly interface for reviewers to view flagged cases, access relevant data, and make decisions.
- **Feedback Mechanisms:** Capture reviewer feedback through categorization, explanations, review time, and agreement metrics.
- **Automated Reporting:** Generate standardized reports for suspicious cases,

Rule Generation with RAG and LLM

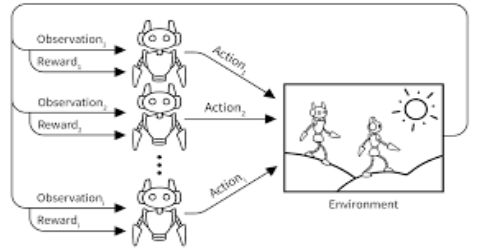
- **Retrieval-Augmented Generation (RAG):** Extract relevant AML regulations and guidelines from websites and internal documents.
- **Large Language Model (LLM):** Generate new rules or refine existing ones based on retrieved information and human feedback.
- **RL Agent Integration:** Update the RL agent's knowledge base with the new or updated rules.

Thank You!

Appendix

RL Policy

ABM	Card	Cheque	EMT & EFT	Cheque
• Cash Indicator • Debit/Credit ratio • Transaction Amount & period • Frequency of Transactions • Duplicate Transactions • Country Risk • Industry Risk Scores • Statistical Features	• Merchant Category • E-commerce Indicator • Transaction Amount • Country Mismatch • Spending Pattern Changes • Frequent Transactions • Industry Risk Scores • Statistical Features	• Transaction Amount • Weekend Transactions • Frequency of Transactions • Quick Succession • Industry Risk Scores • Statistical Features	• Transaction Amount • Weekend / Late-Night Transactions • Industry Risk Scores • Statistical Features • Frequency of Transactions	• Transaction Amount • Weekend Transactions • Frequent Large Transfers • Industry Risk Scores • Statistical Features



CUSTOMERS TO INVESTIGATE

8%	15.3%	1.3%
IDENTIFIED BY ANOMALY DETECTION	**IDENTIFIED BY EMBEDDINGS**	**HIGHLIGHTED BY RL**
The combined list of all outliers from multiple methods of clustering	Combination of clustering and embeddings	Further investigation for human review