Case Study: Extracting Insights for Fraud Detection



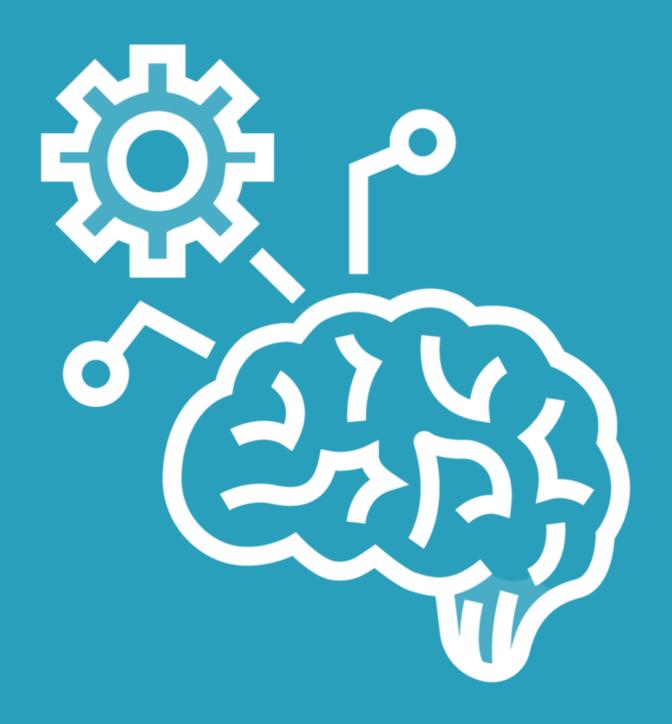
Janani Ravi Co-founder, Loonycorn

www.loonycorn.com

Overview

Case Study: Artificial Intelligence Enabled Financial Crime Detection

Towards Artificial Intelligence Enabled Financial Crime Detection



Background and Context

Exploring current techniques for the detection of money laundering

Money Laundering

Illegal process of concealing the source of money which has been obtained through criminal activities and putting this money into legitimate financial systems

Increased Money Laundering Risk



Growing use of digital channels and invention of digital money such as Bitcoin

Amount of money transferred using money laundering estimated to be between 2% - 5% of overall GDP throughout the world

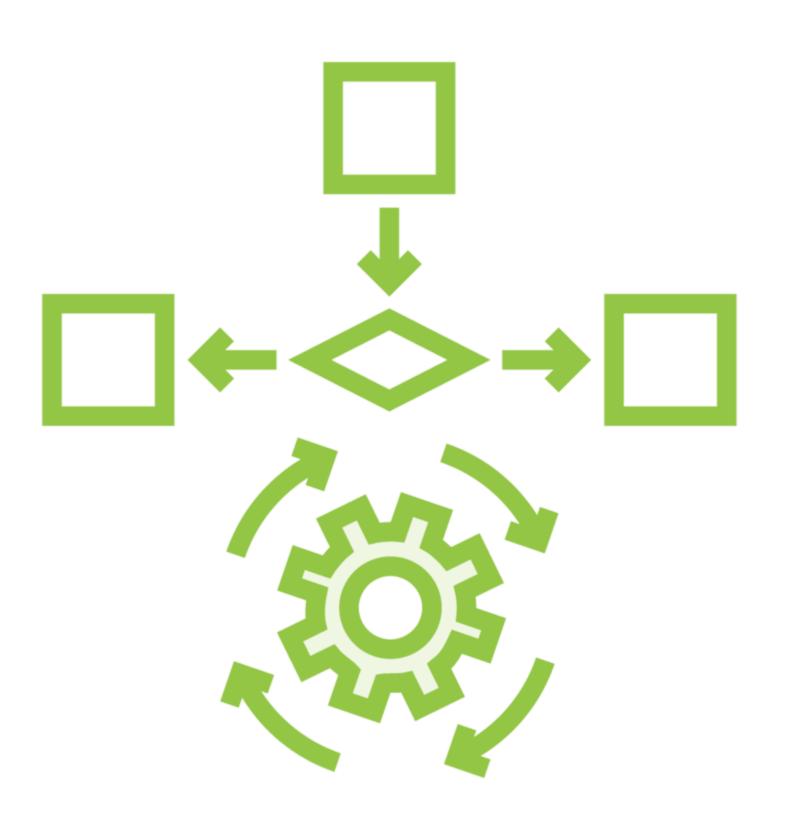
Categories of Anti-money Laundering Models

Clustering Rule-based Classification **Anomaly Detection**

Categories of Anti-money Laundering Models

Rule-based

Rule-based Models

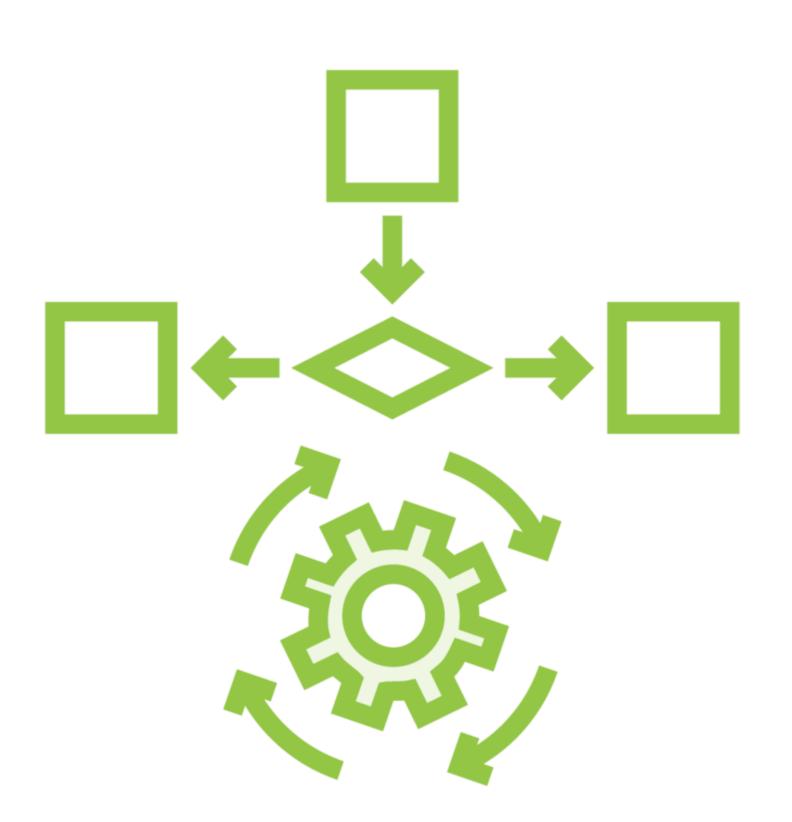


Initial step at financial institutions

Use pre-defined rules and thresholds to detect unusual transactions

- Transactions above a certain amount
- Transactions originating in black-listed country
- Transactions that include specific words
- Repeated transactions to an account

Rule-based Models

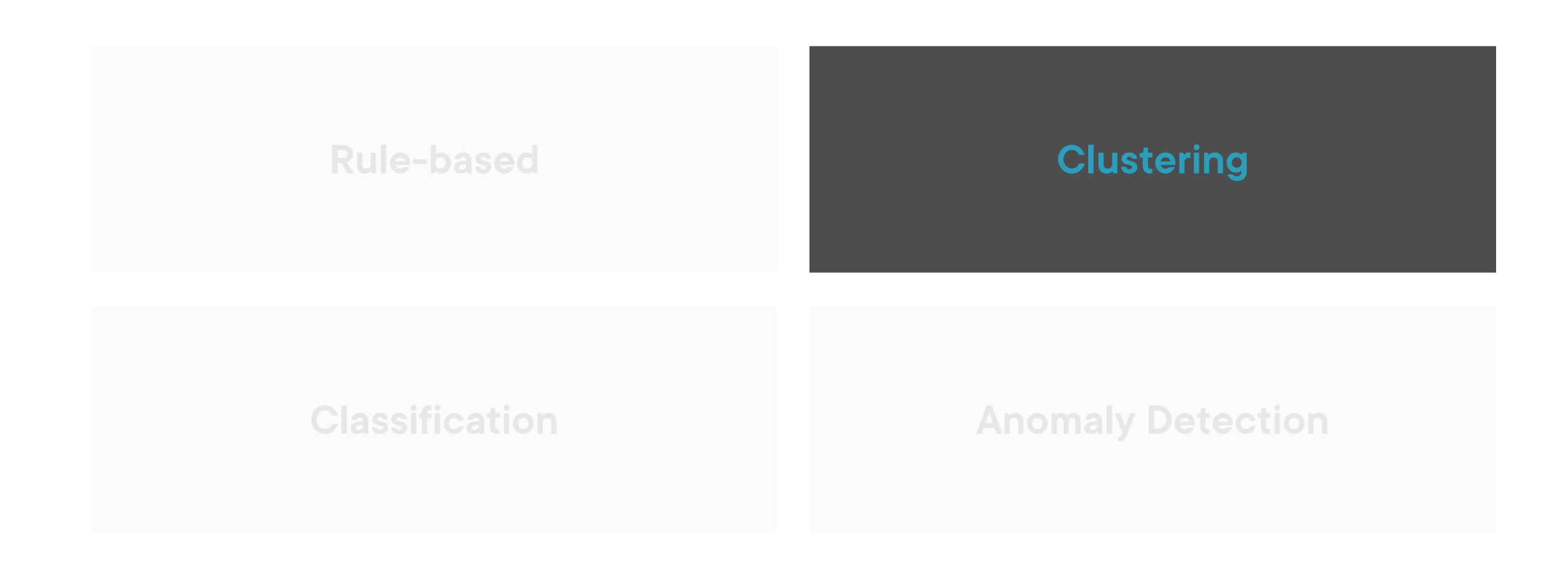


Suspicious transactions detected using statistical rules

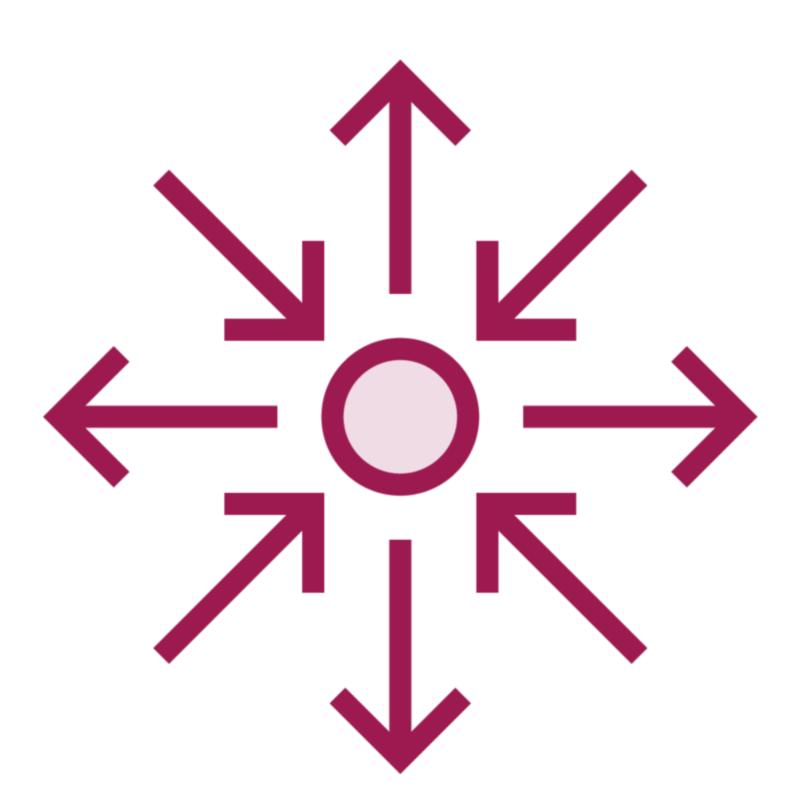
Compare features such as amount and frequency with average

If deviation is above a certain amount flag as suspicious

Categories of Anti-money Laundering Models



Clustering



Apply clustering or grouping to transactions

Investigate each cluster

Identify outliers

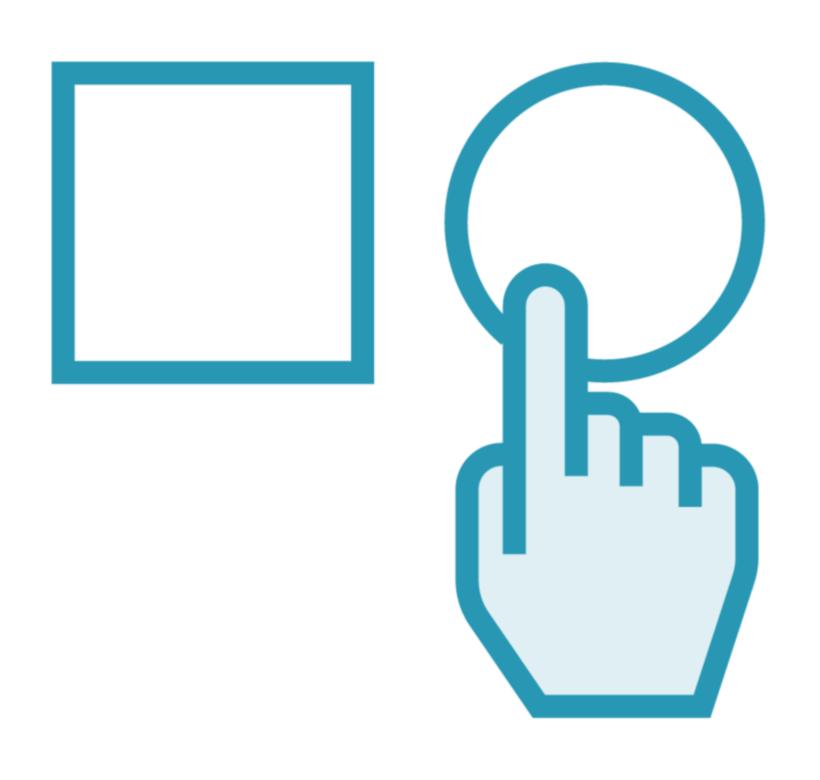
K-means clustering a popular algorithm

Original k-means not successful at detecting outliers

Categories of Anti-money Laundering Models

Classification

Classification



Preprocess transaction data by labeling as suspicious or not

Create feature vector of transaction attributes

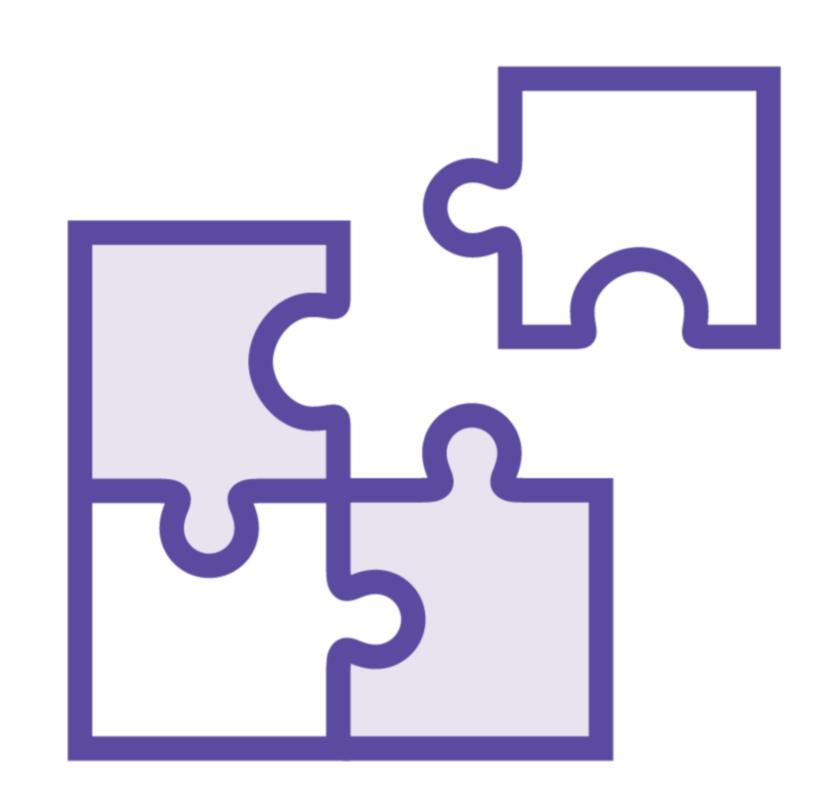
Traditional models - SVMs, Logistic Regression, Random Forest

Neural network models

Categories of Anti-money Laundering Models

Anomaly Detection

Anomaly Detection



Identify transactions that deviate from the usual behavior

Unexpected transactions

Similar to advanced rule-based models that use statistical parameters

Transactions which deviate from the average flagged as suspicious

Anomaly Detection

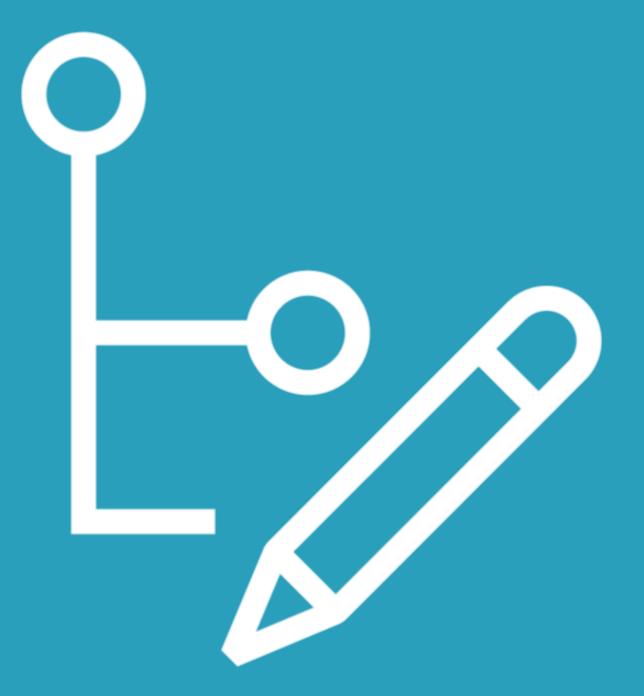


Isolation forest (iforest) an ML algorithm for anomaly detection

Uses a tree structure to fit on data

Leaf nodes deep in the tree unlikely to be outliers

Leaf nodes close to the root more likely to be outliers



Features Used in AML

Transaction features and customer features

Types of Features Used in AML

Transaction Features

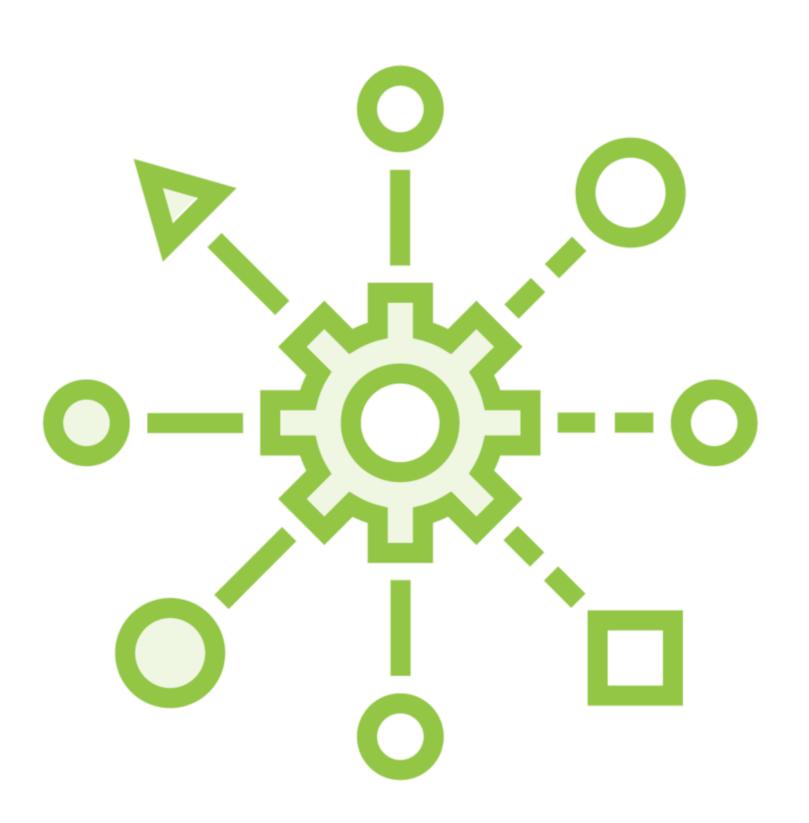
Customer Features

Types of Features Used in AML

Transaction Features

Customer Features

Transaction Features



Attributes associated with the transaction itself - not with the sender or receiver

No data privacy or compliance issues

Transaction Features



Time of transaction

Origin and destination

Amount

Accumulated fund flow

Type of transaction - money transfer, wire transfer, cash

Types of Features Used in AML

Transaction Features

Customer Features

Customer Features

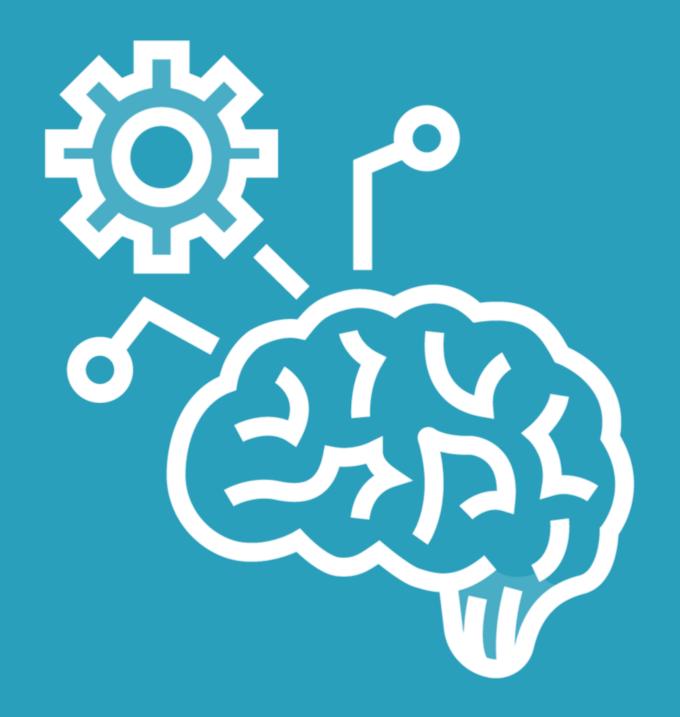


Attributes associated with the customer involved in the transaction

Involve collecting data on customers and their transactions and building profiles

Categorizing customers in predefined risk categories

Data may need to be anonymized or masked to deal with privacy issues



Data Labeling

Snorkel model for data labeling

Data Labeling



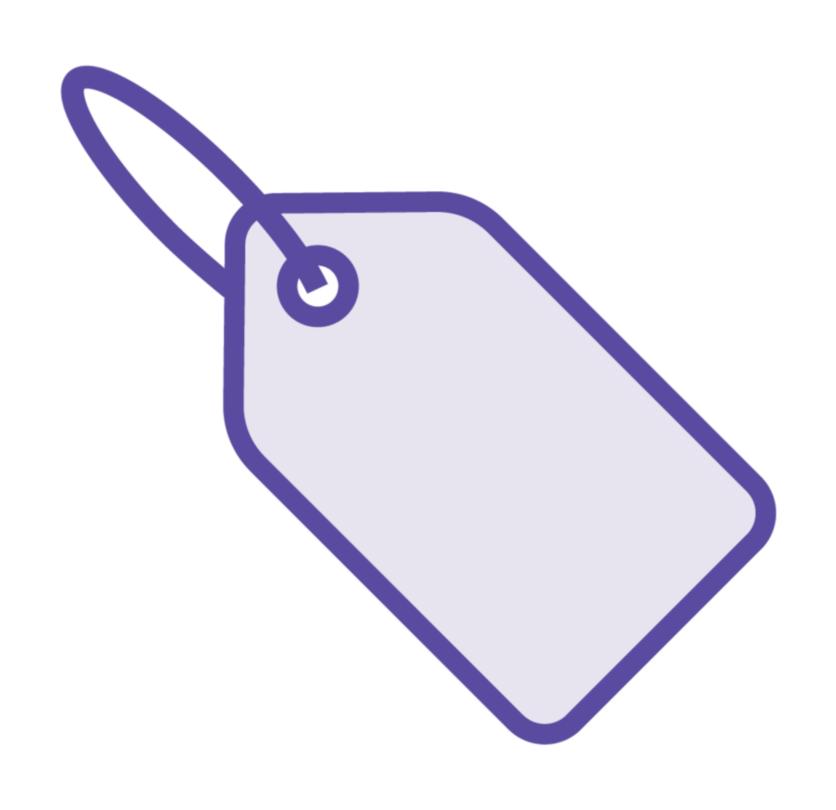
A critical pre-processing step before fitting an ML model

Hand-labeling data is expensive and time consuming

Hire large groups of people to label data

Use crowd sourcing to label data

Different labeling sources might label data in a conflicting manner

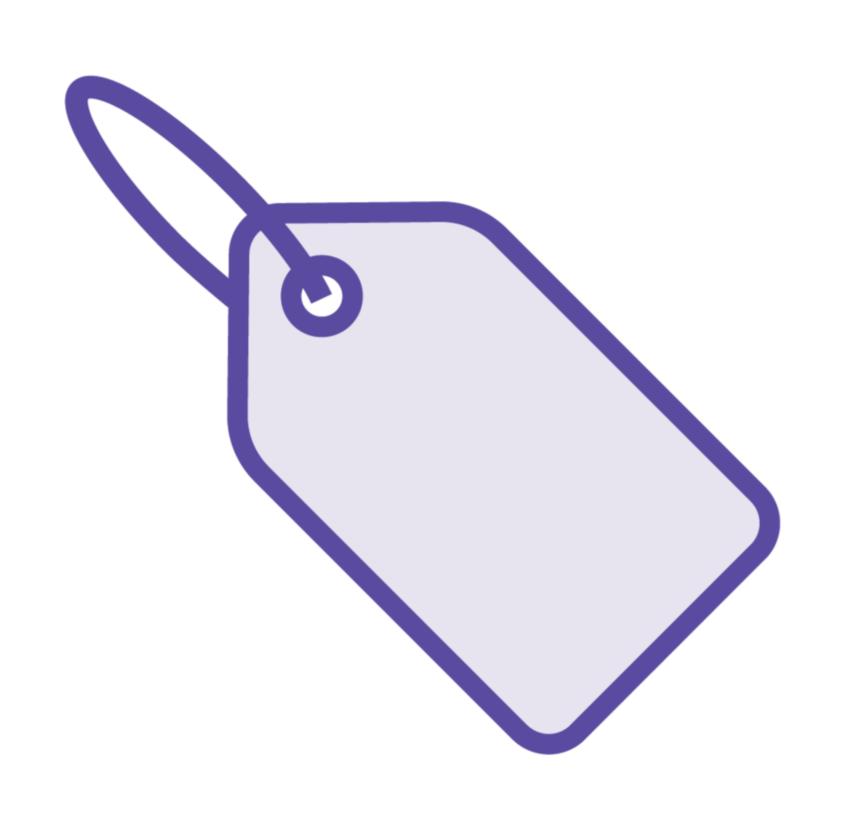


An ML model for labeling developed at Stanford University

Uses several labeling functions developed by subject matter experts

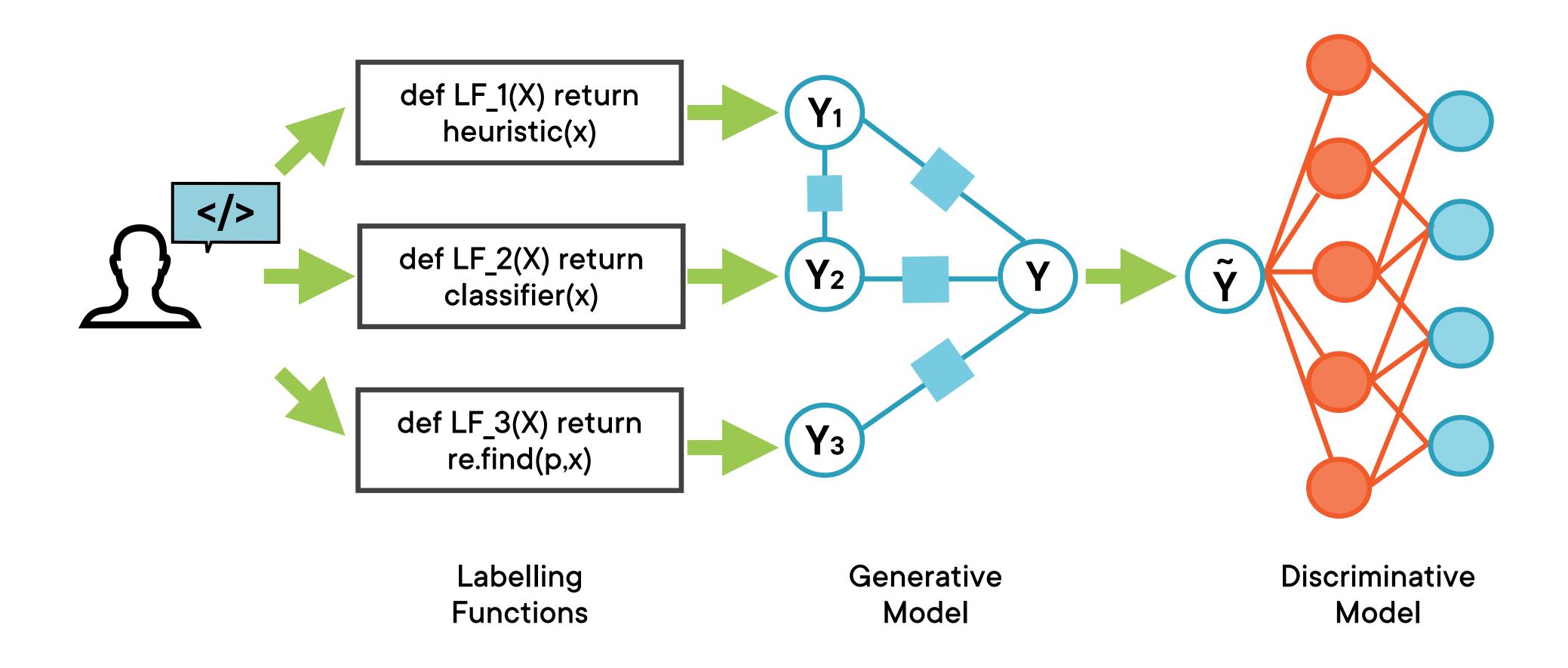
Model determines weight of each labeling function

Based on agreements and disagreements between labels for data points

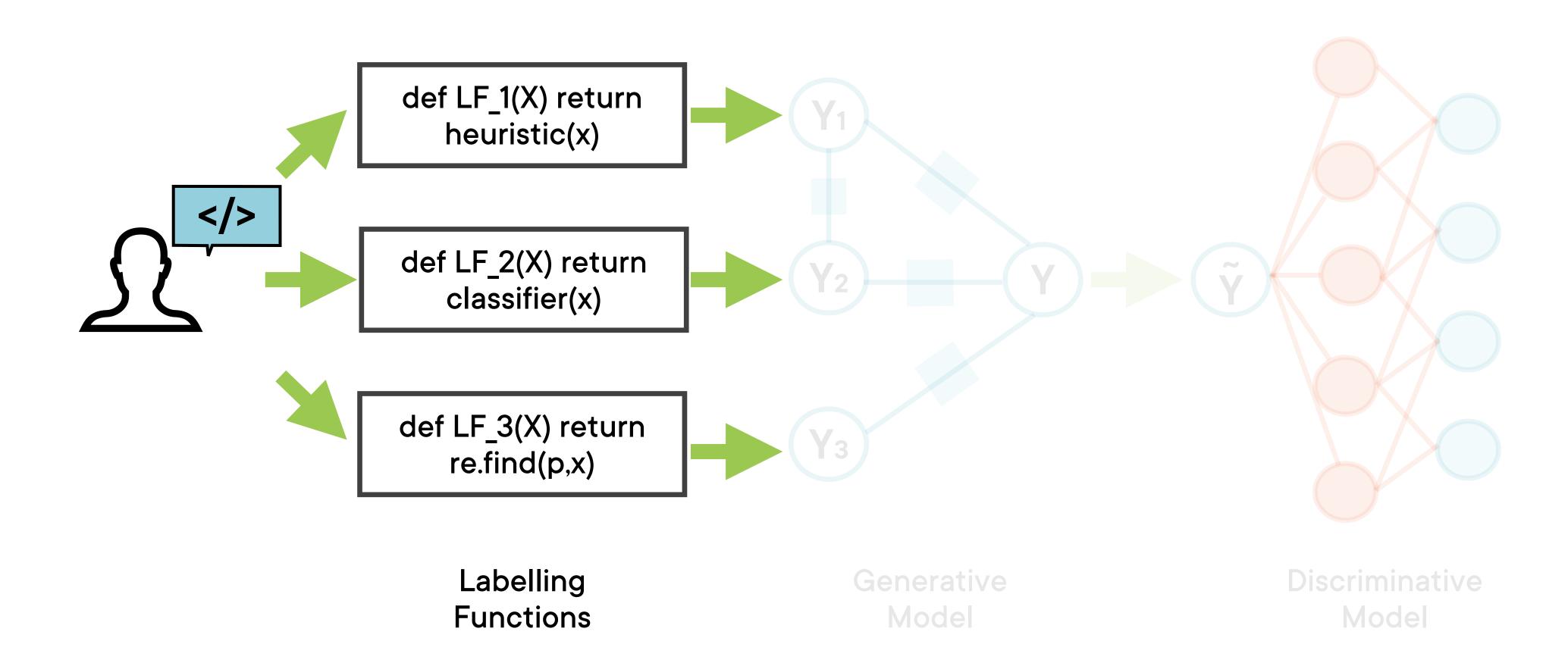


Snorkel uses labels from weak supervision sources i.e. the labeling functions

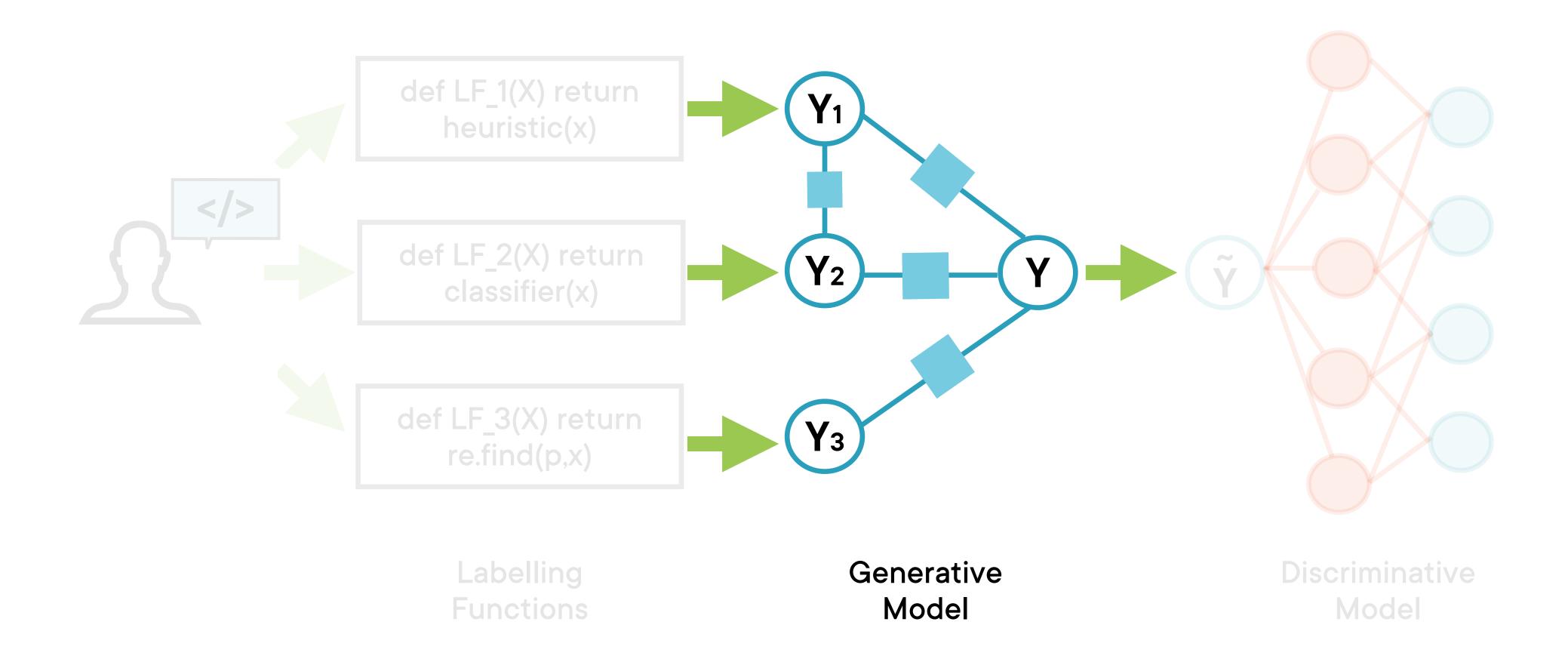
Outputs probabilistic labels which are then used to train classifiers



Weak Supervision Sources

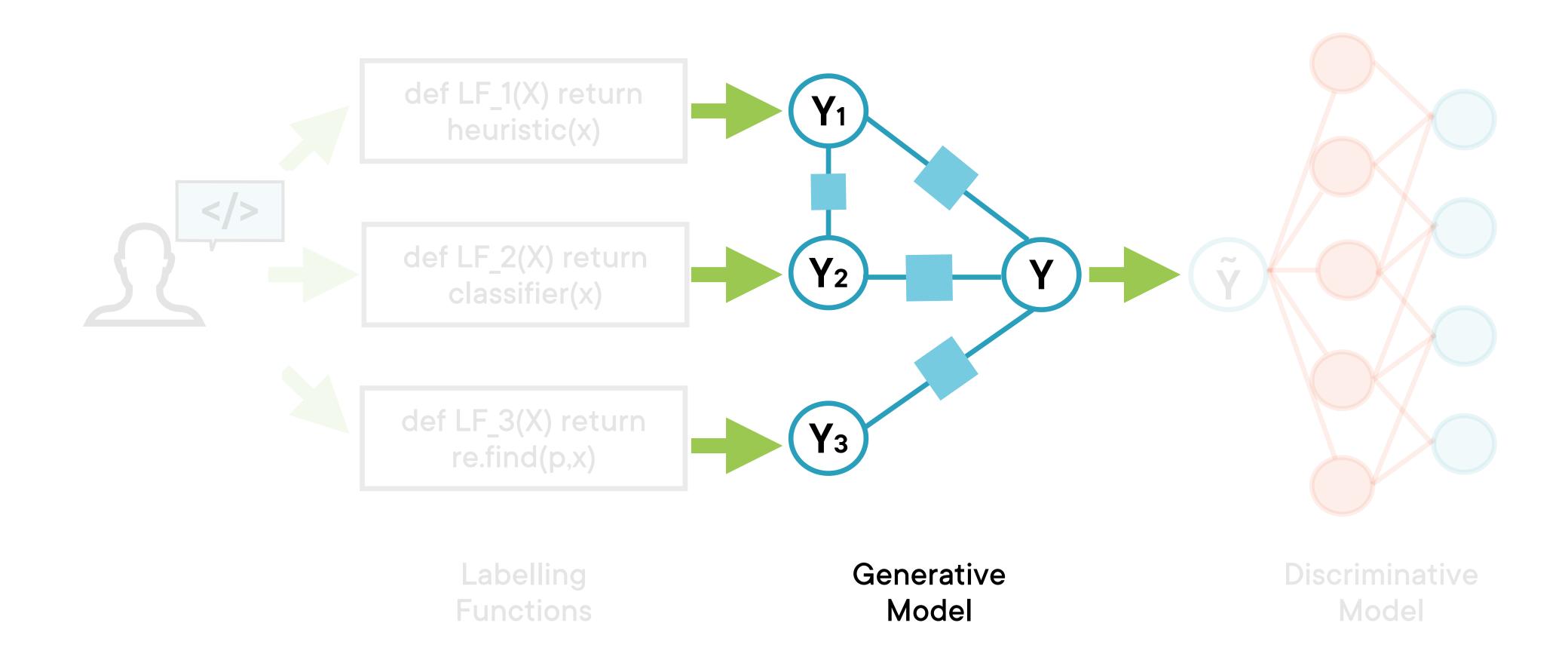


Generative Model



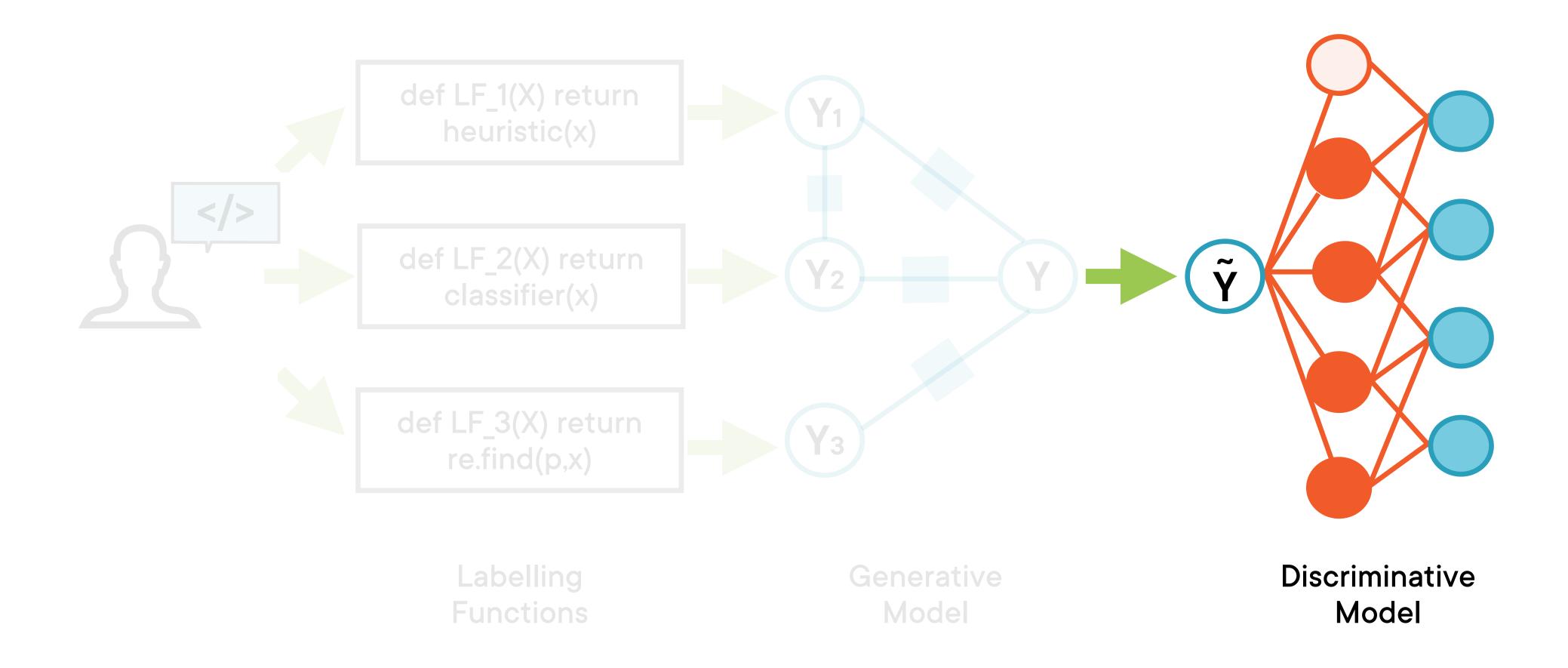
Use labeling functions' correlations i.e. whether they agree or disagree

Generative Model

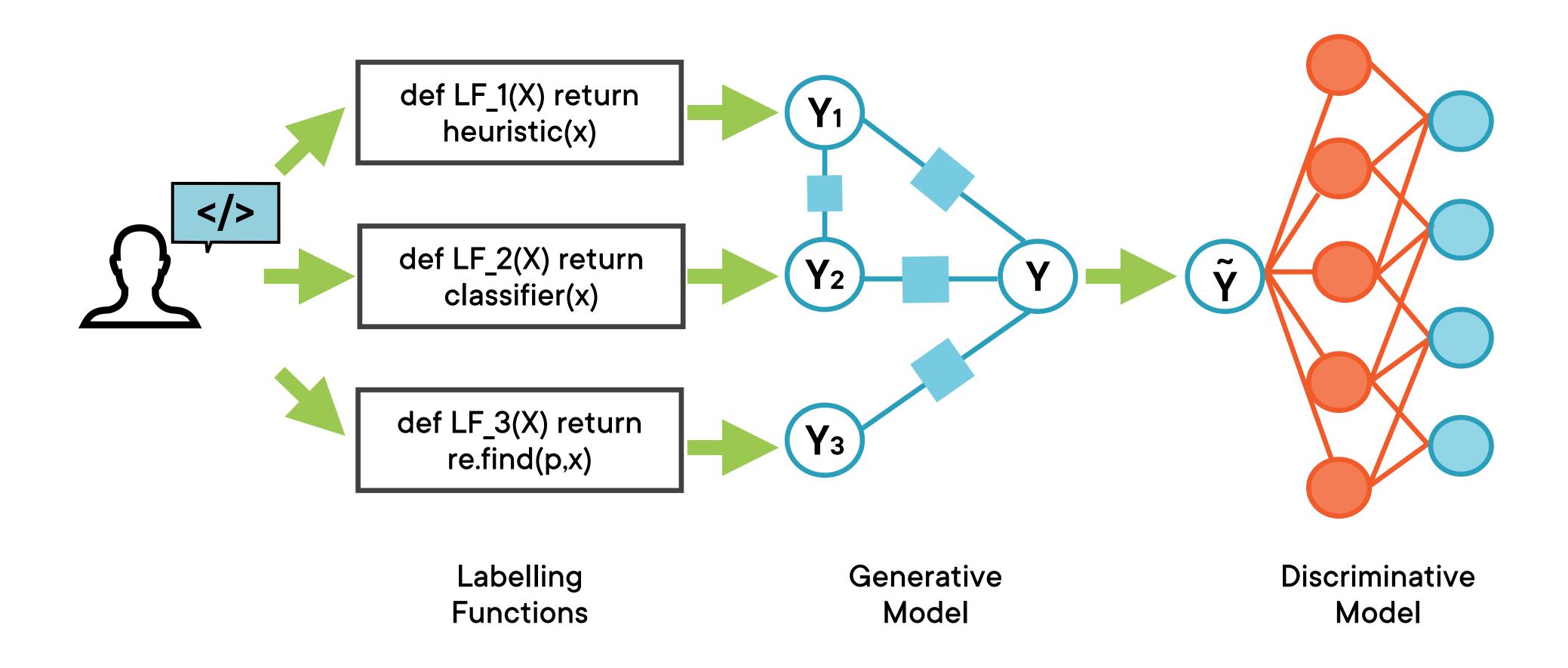


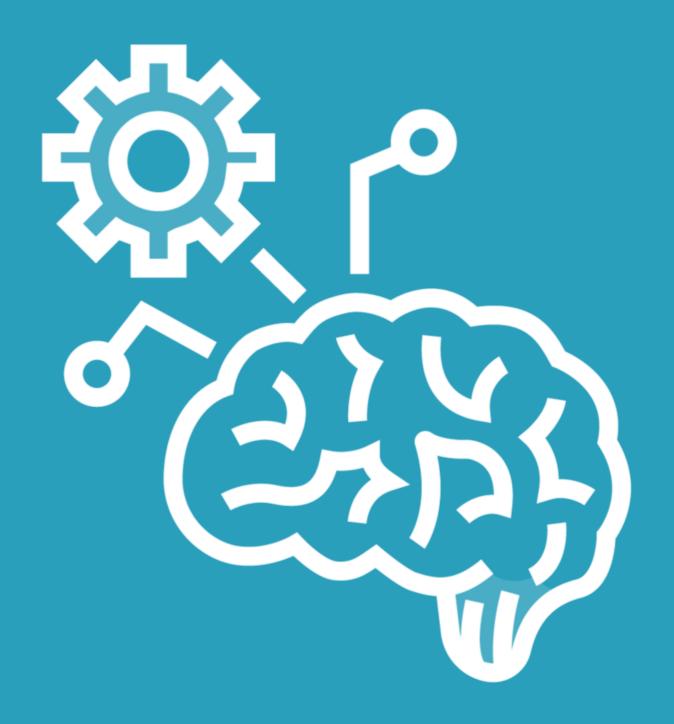
Majority voting, model accuracies

Train a Discriminative Model



Generalize beyond the noisy generative model

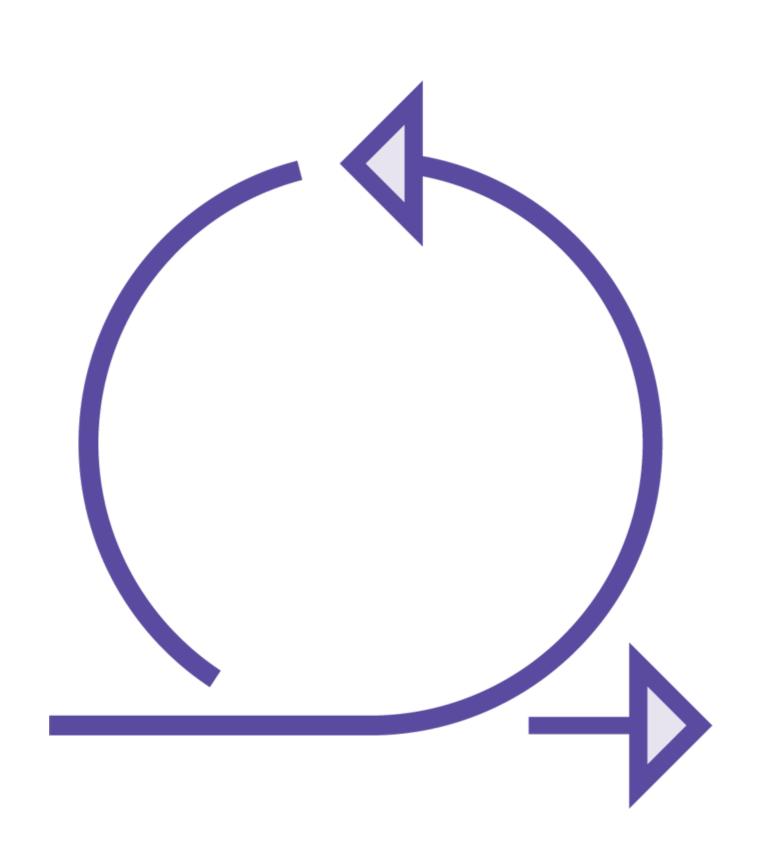




Methodology and Model

Discuss methodology to detect and prevent money laundering, walk through model steps, evaluate results

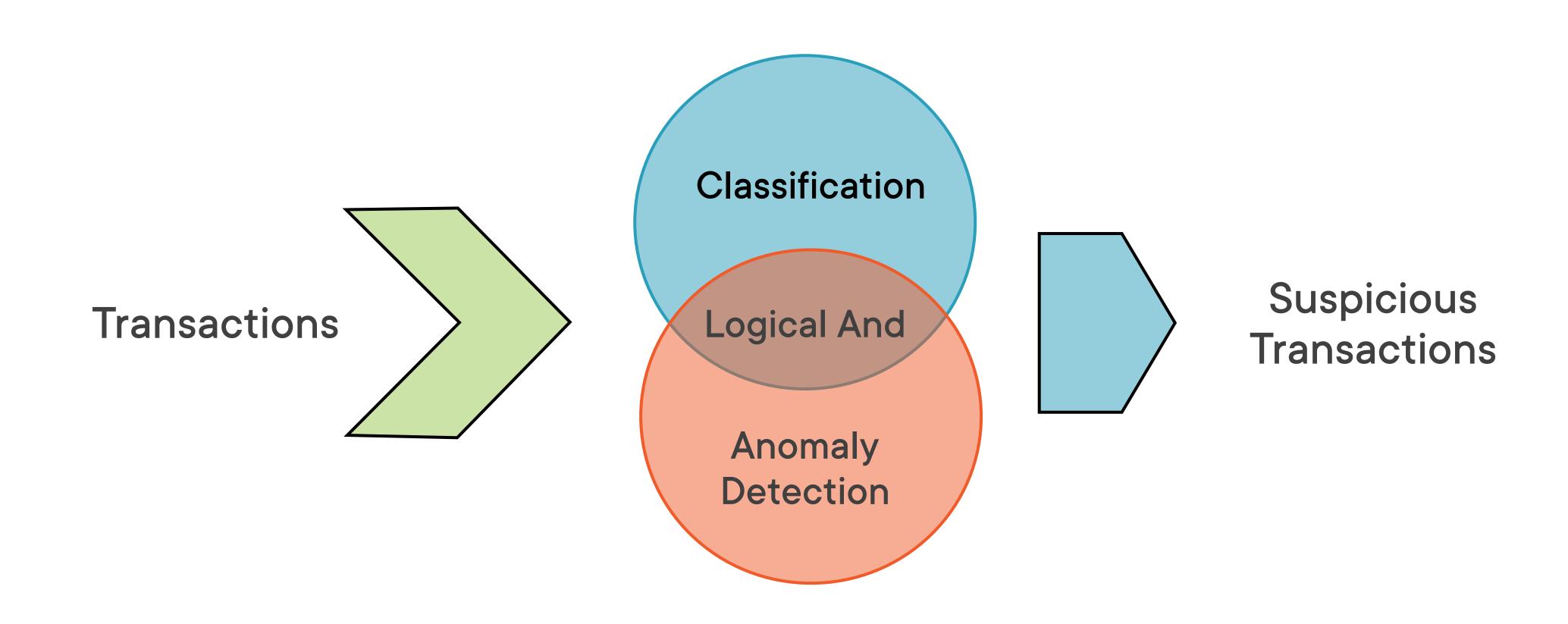
Intelligent Hybrid Pipeline



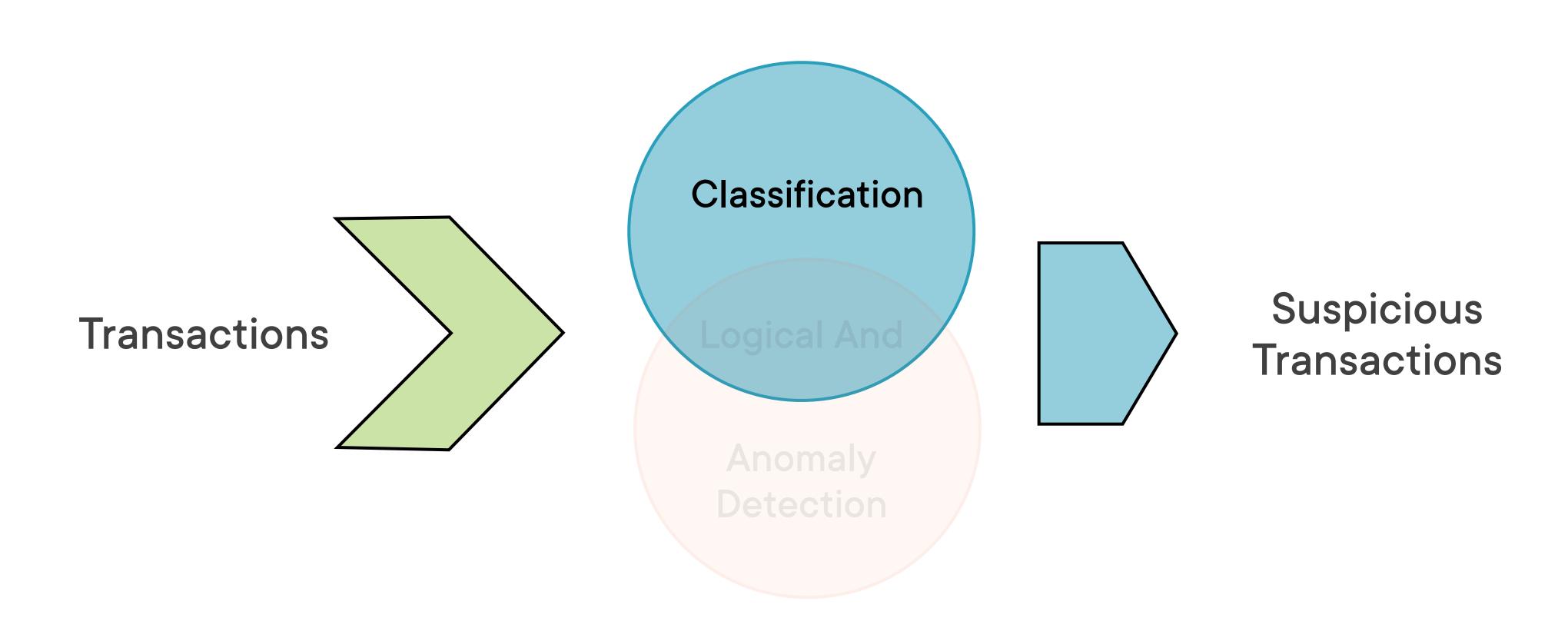
Includes both supervised and unsupervised learning approaches

Classification + Anomaly detection

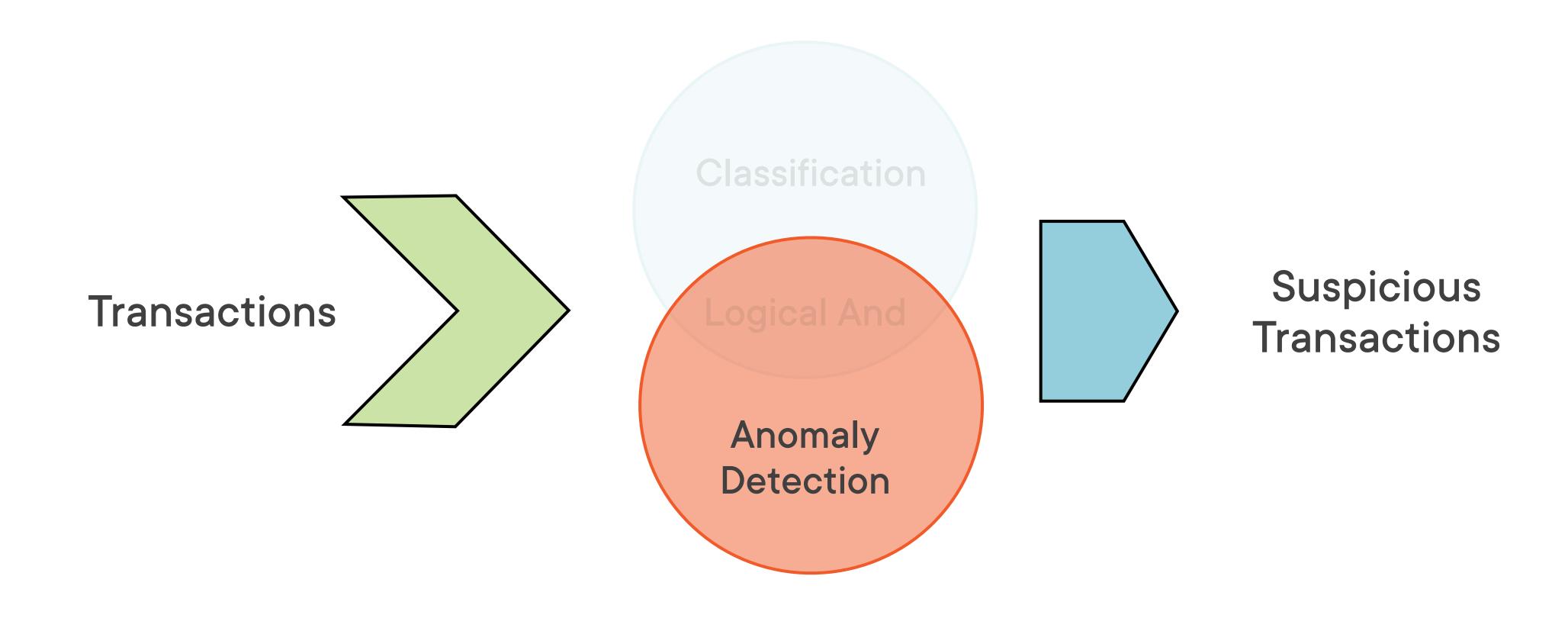
Intelligent Hybrid Pipeline



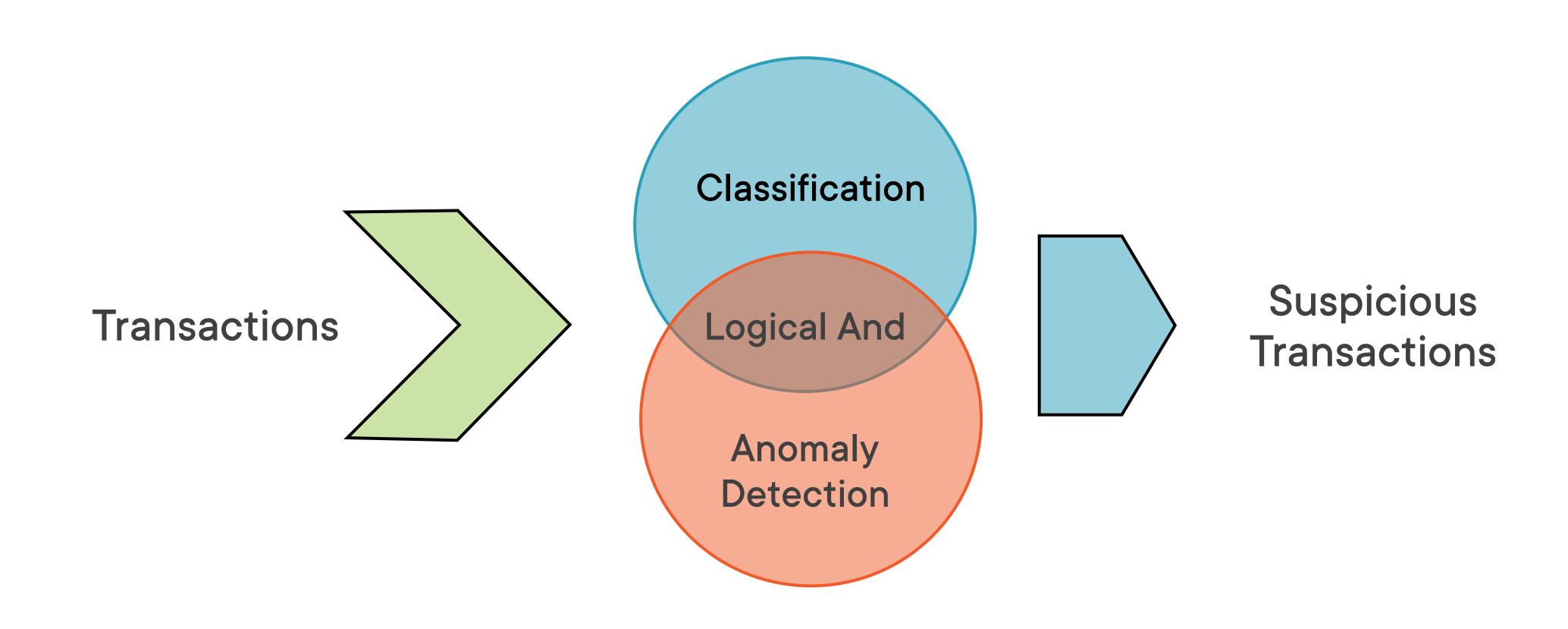
Classification Model to Detect Suspicious Transactions



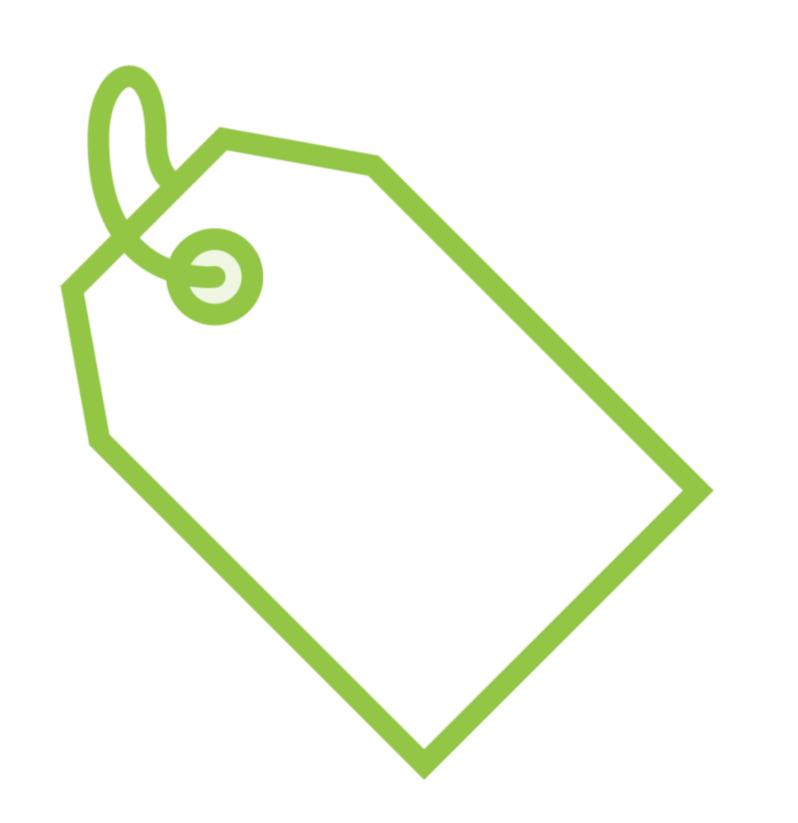
Anomaly Detection to Capture Unusual Transactions



Logical AND to Improve Accuracy and Minimize False Positives



Snorkel for Data Labeling

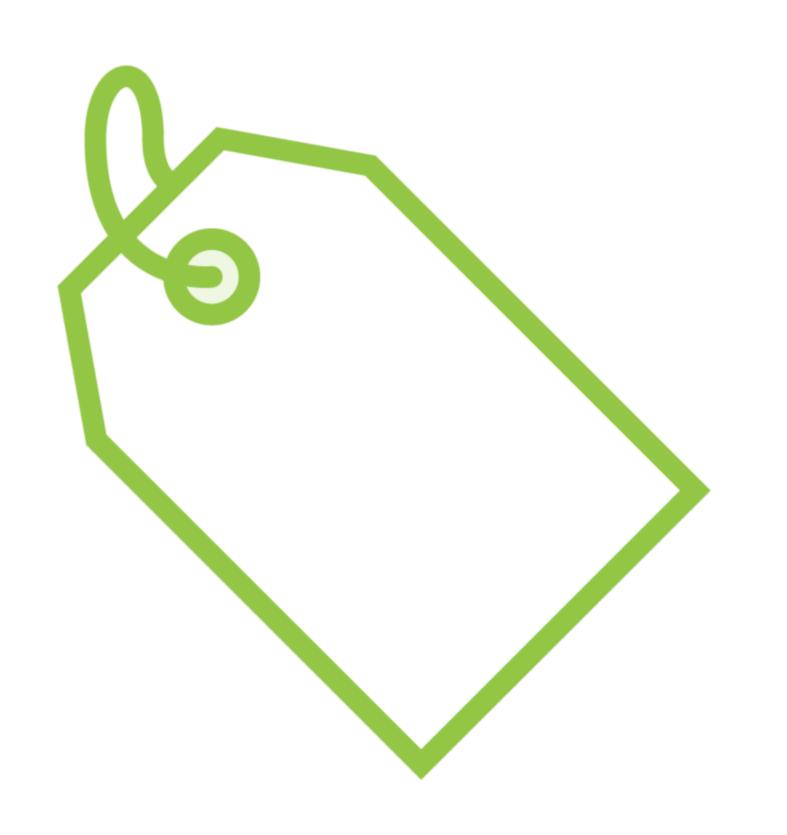


Dataset contains a total of 100,000 records

Experts to label 10% of this data

Snorkel model for the rest

Simple Rules for Labeling Functions

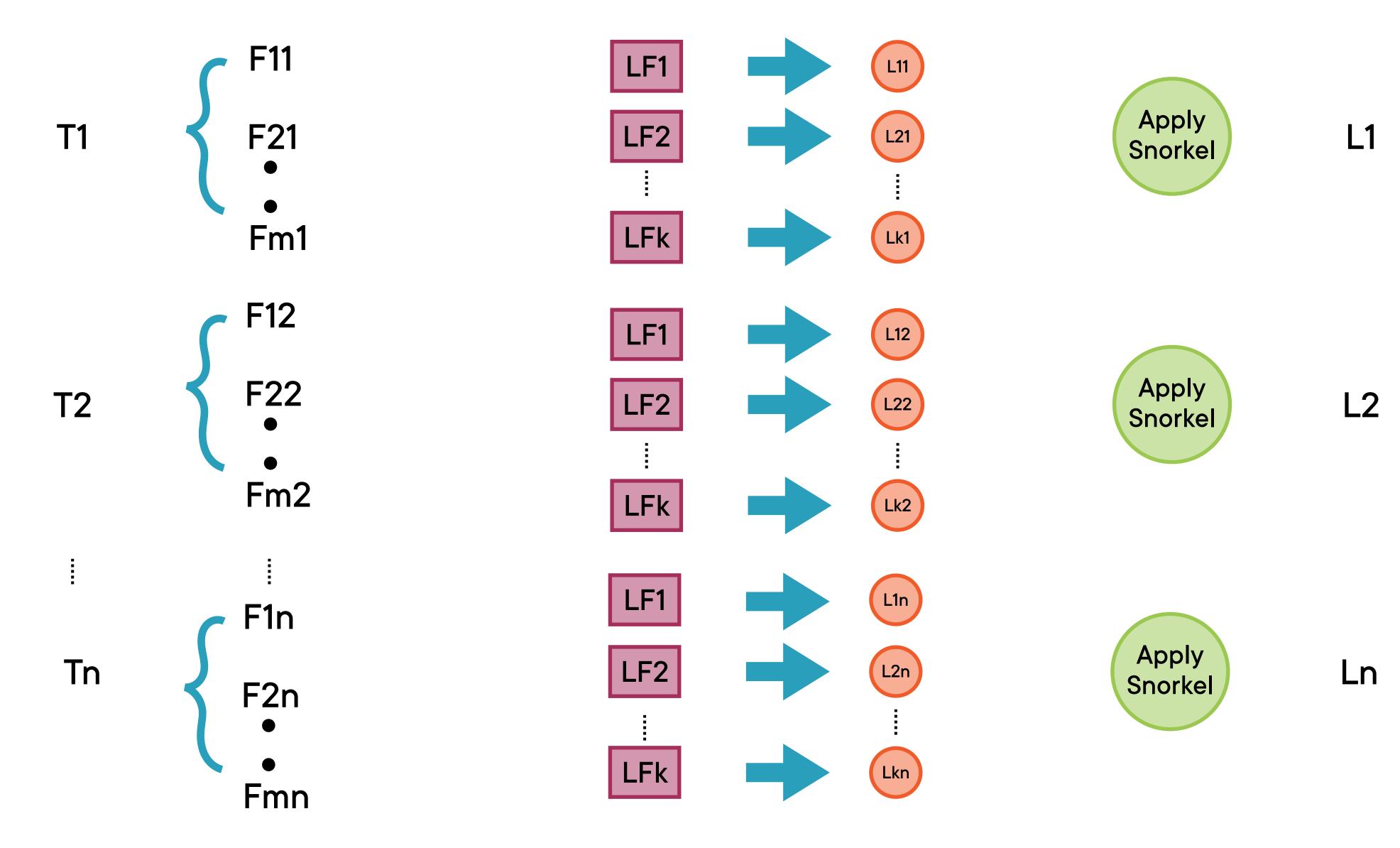


If cash transaction for > 10000 = suspicious

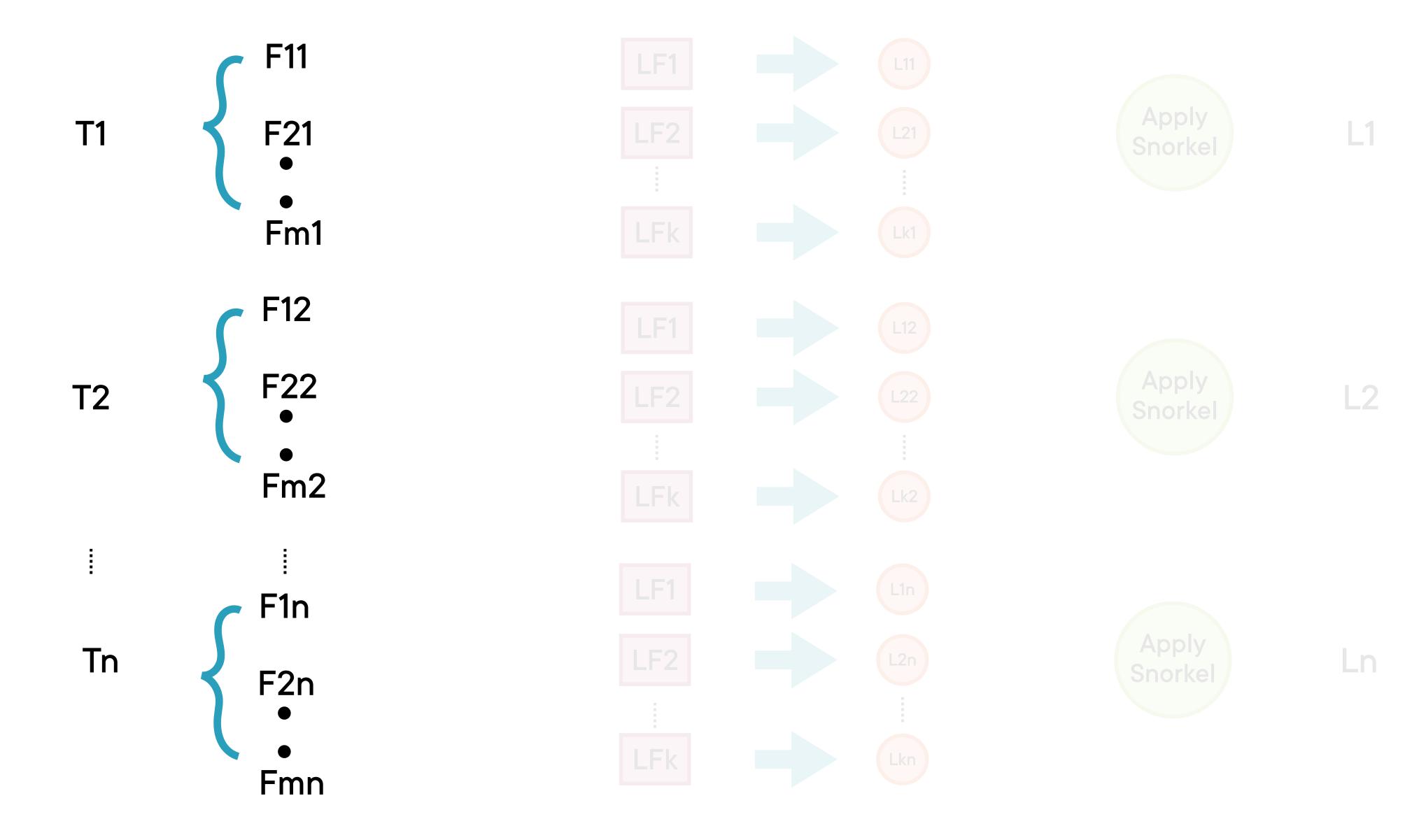
If source country blacklisted = suspicious

If transaction category includes special words = suspicious

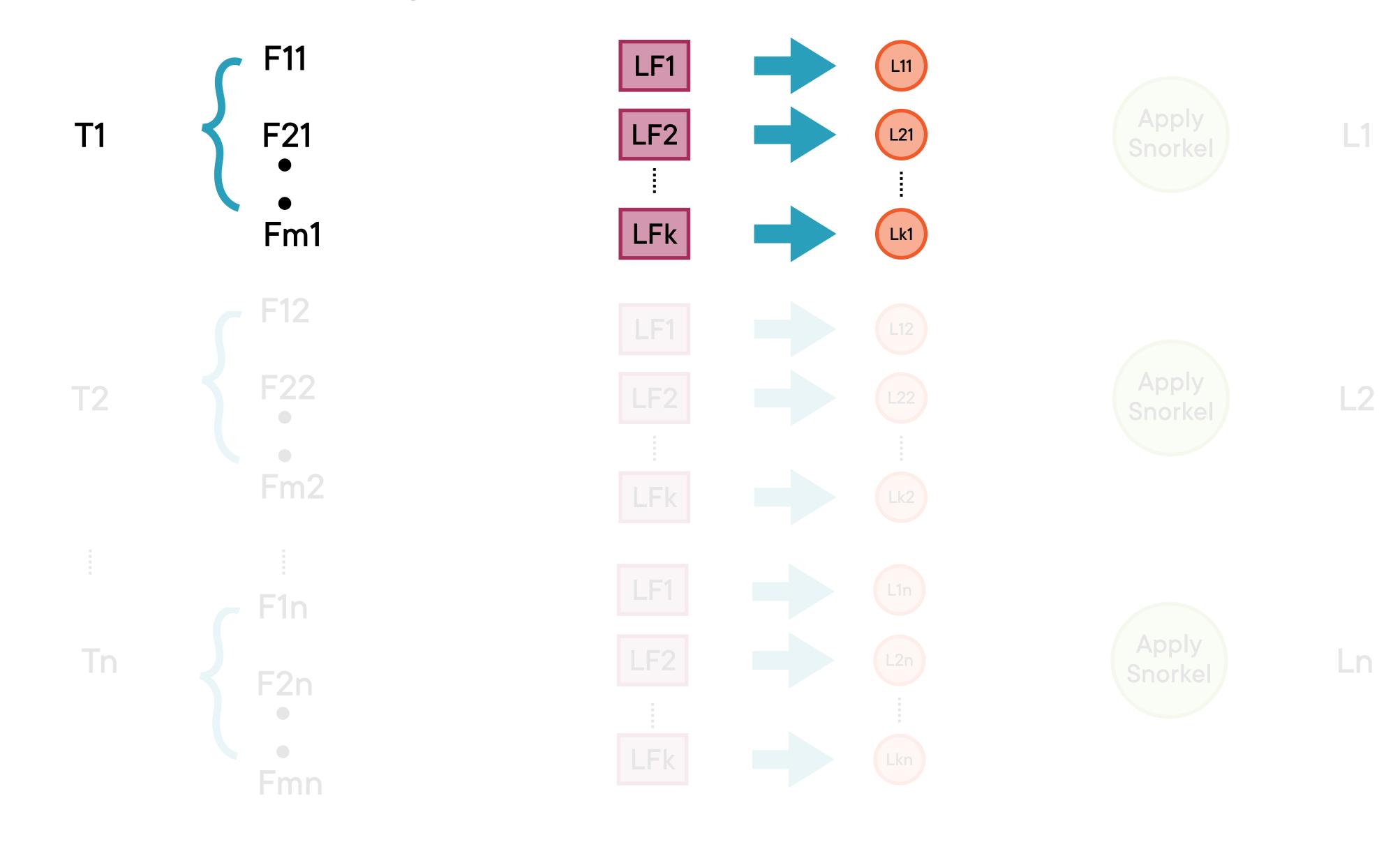
Snorkel for Data Labeling



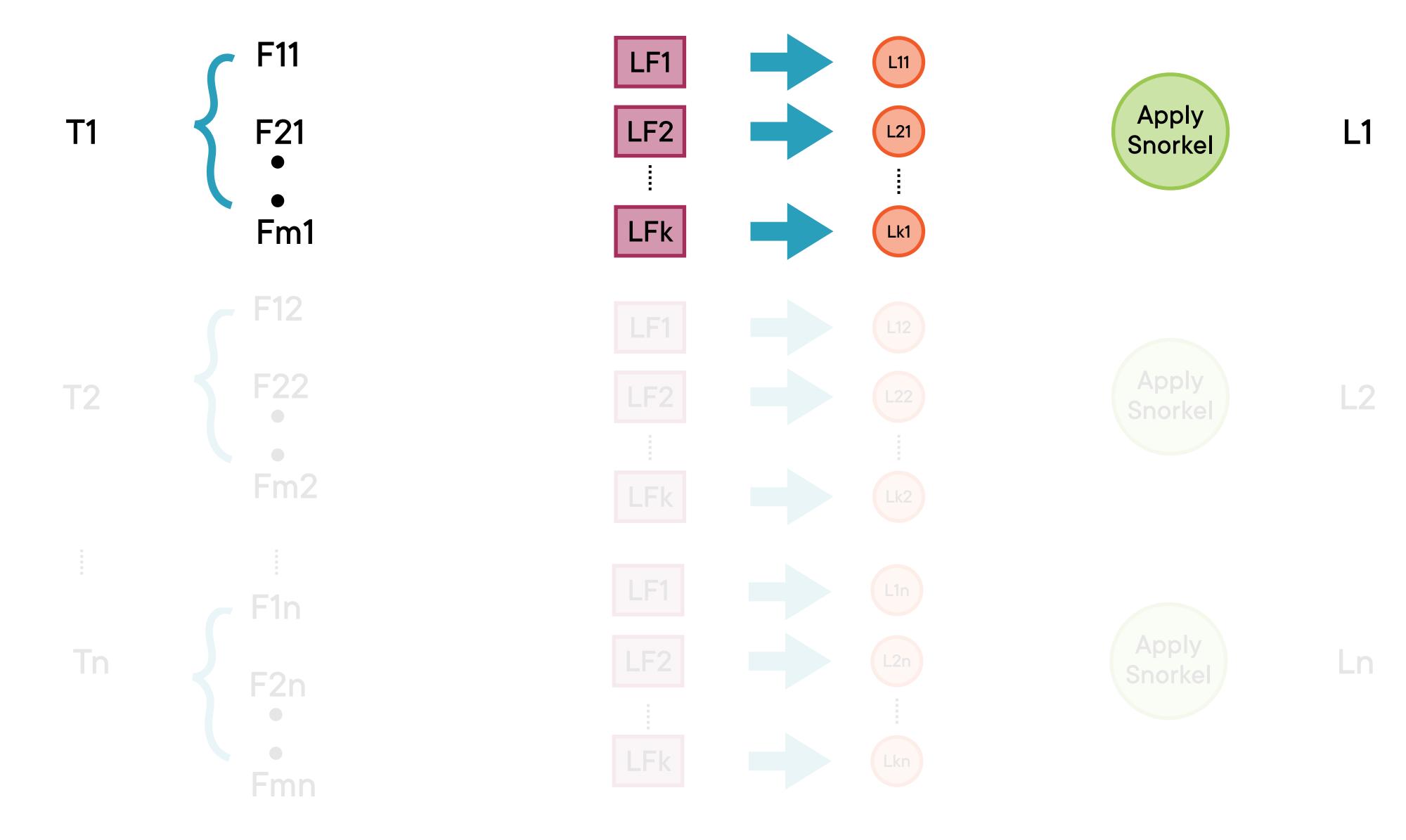
Transaction Features



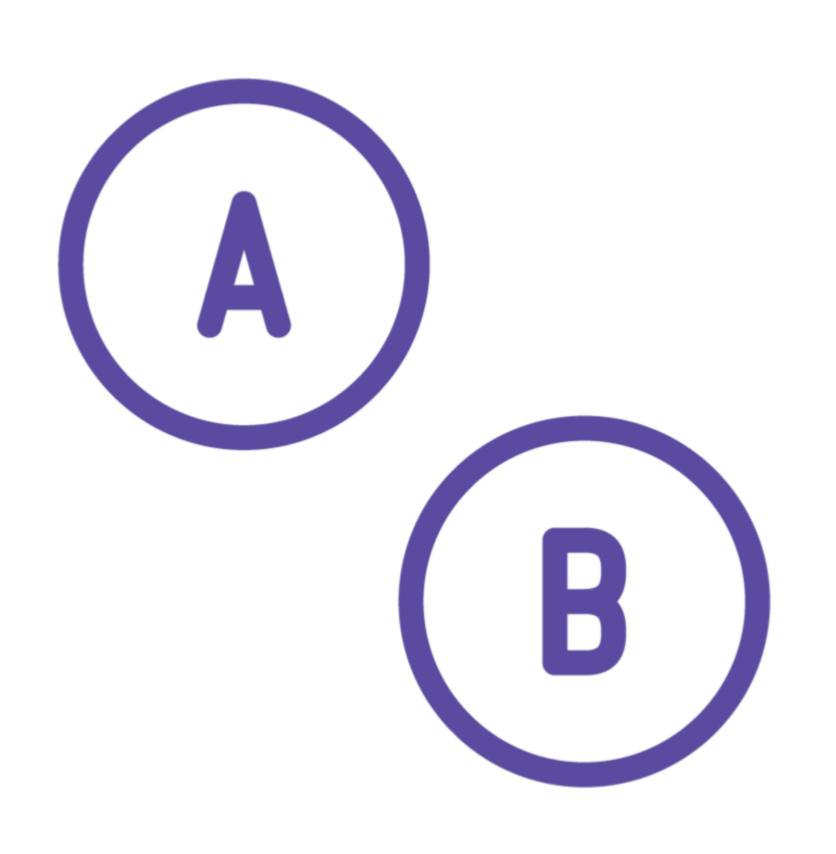
Apply Labeling Function to Each Transaction



Snorkel Decides a Single Label



Classification Model

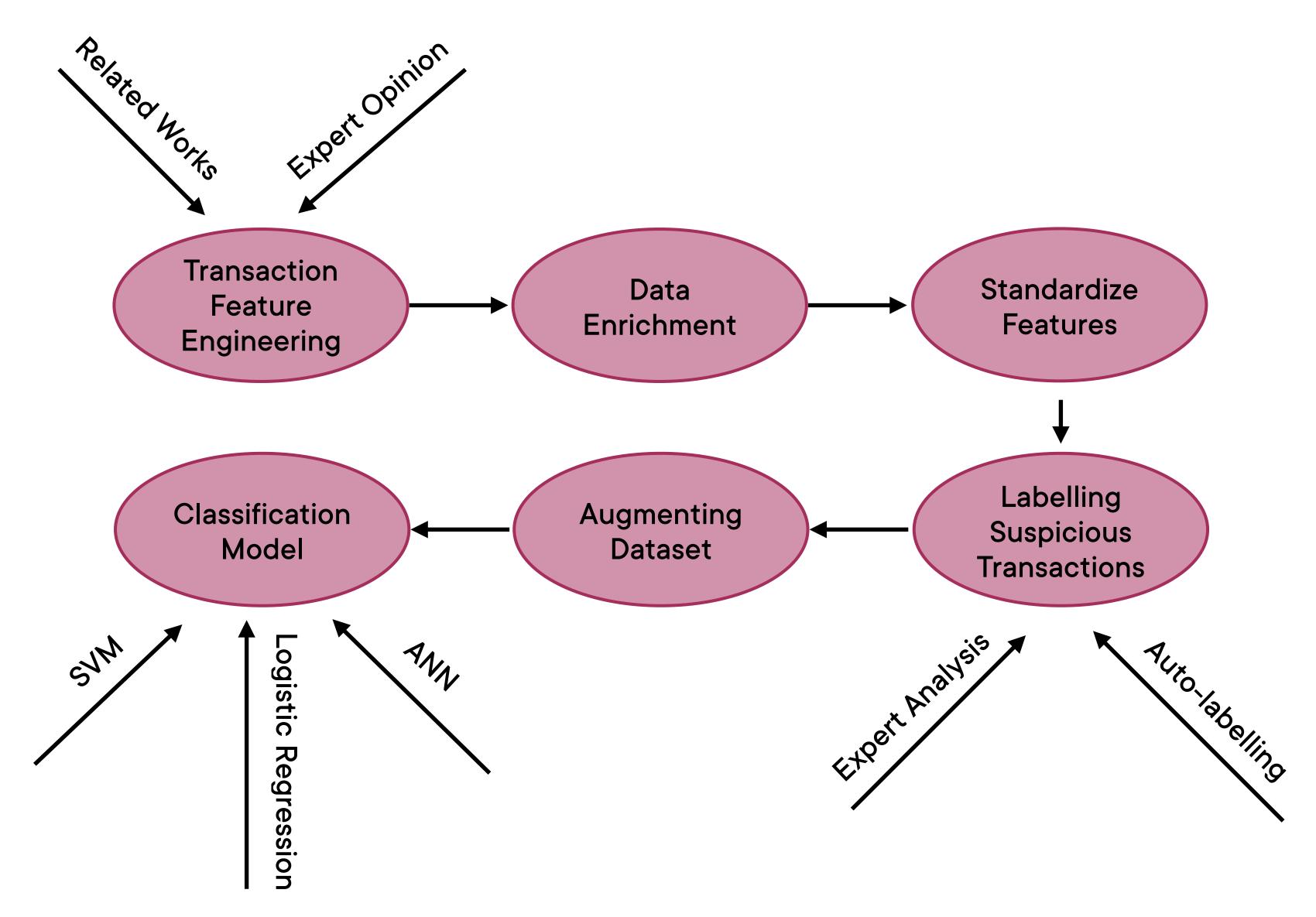


Binary classification to predict suspicious transactions

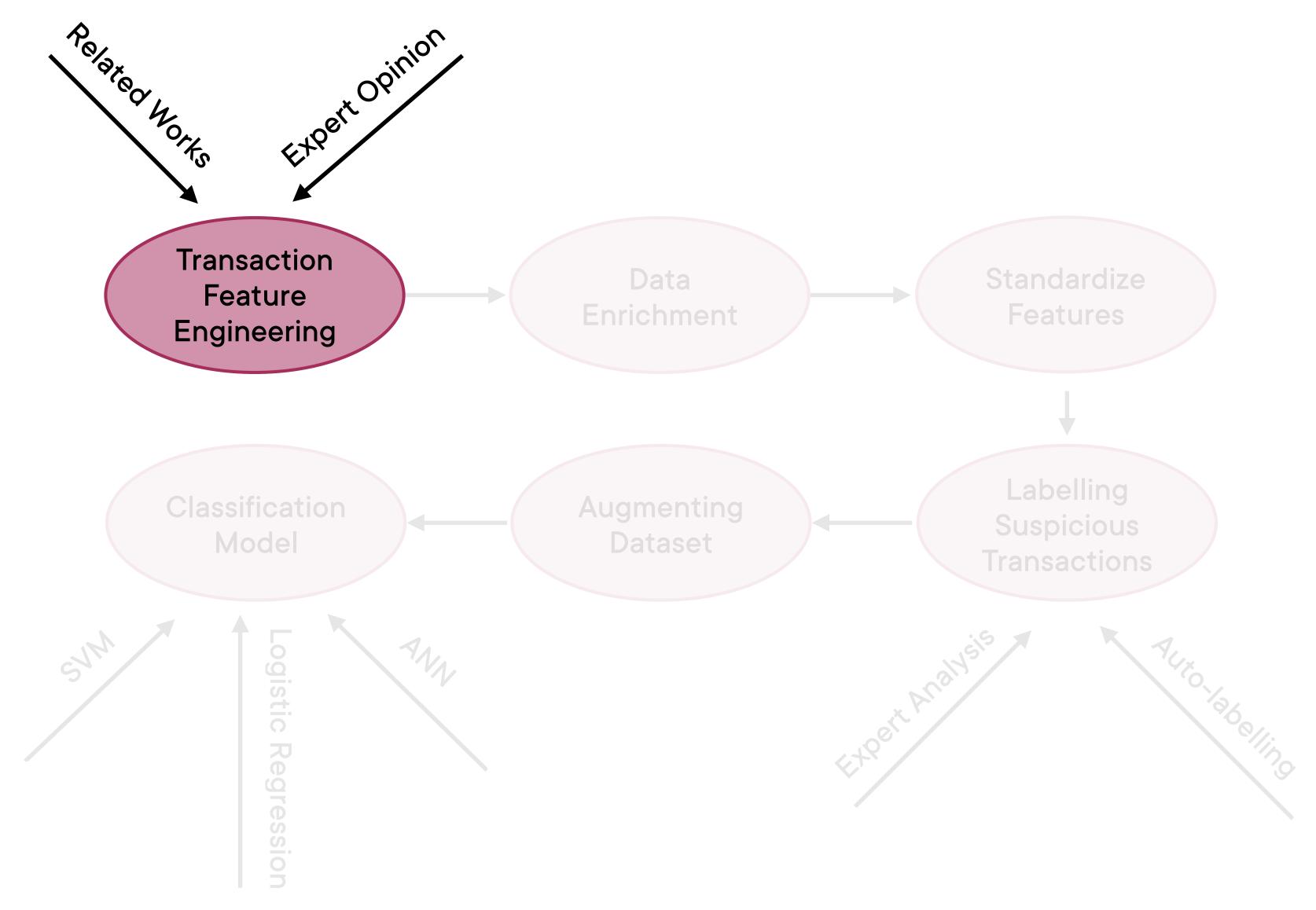
Label 1 = suspicious

Label 0 = Not suspicious

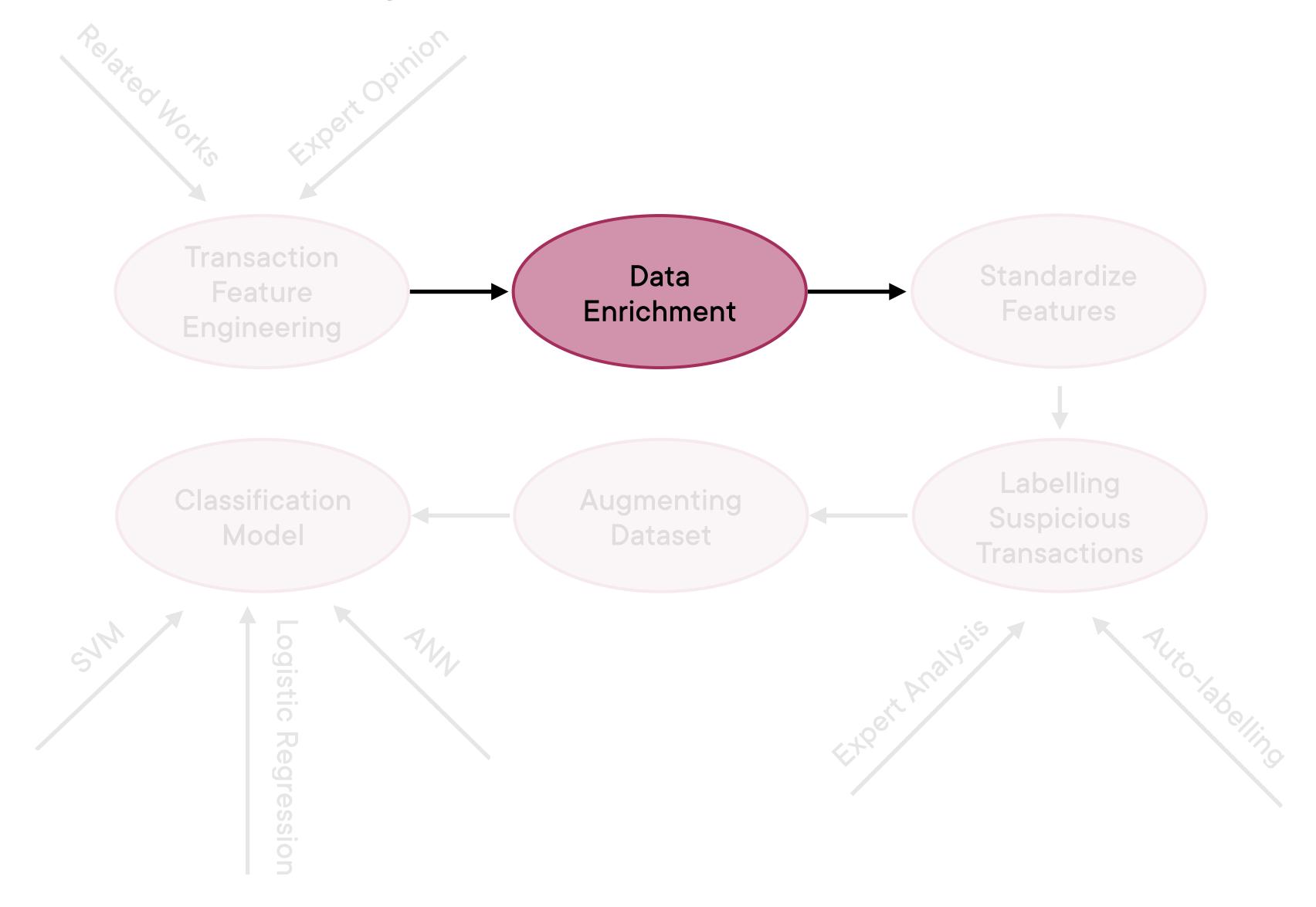
Classification Model



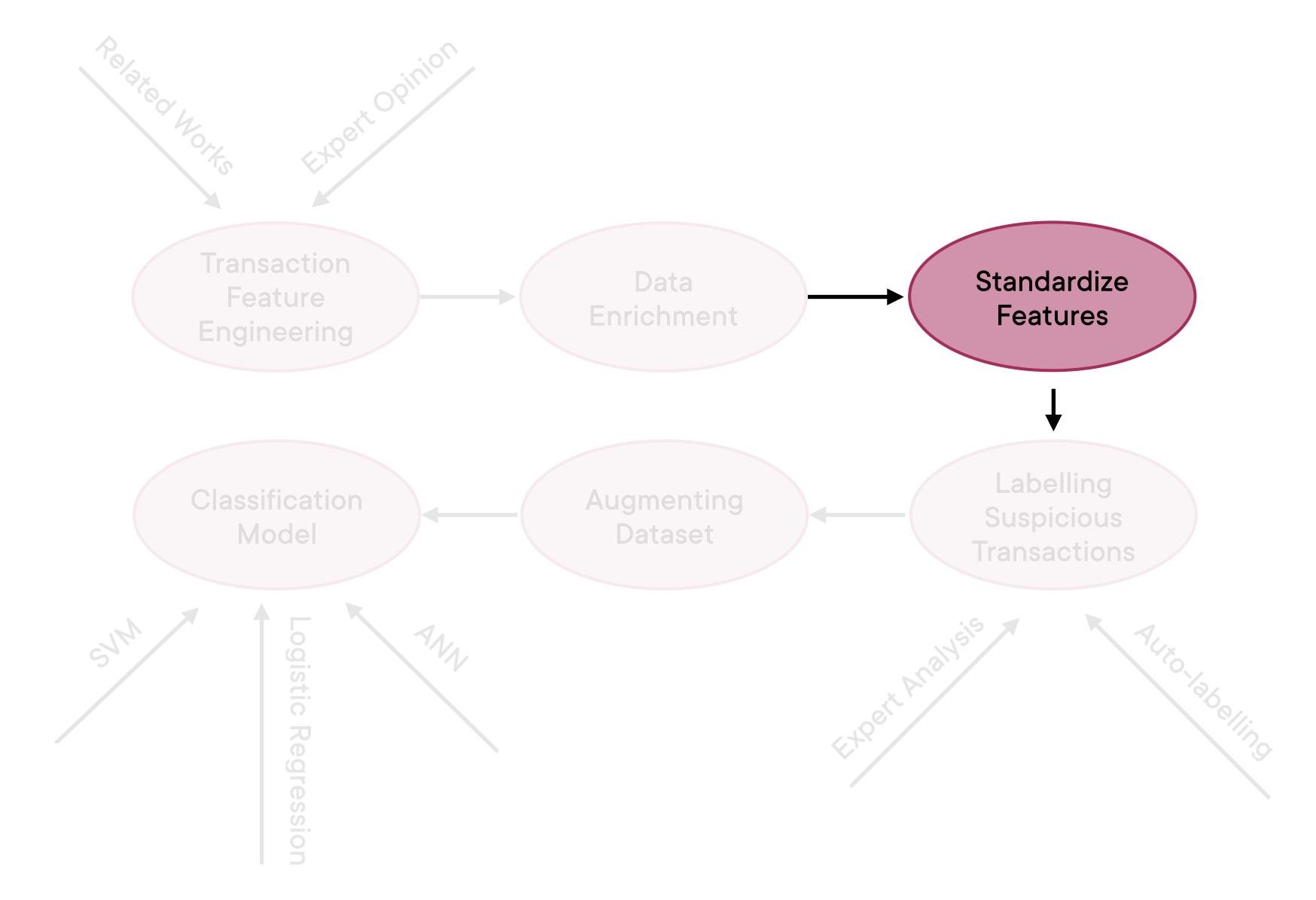
Selecting Important Features



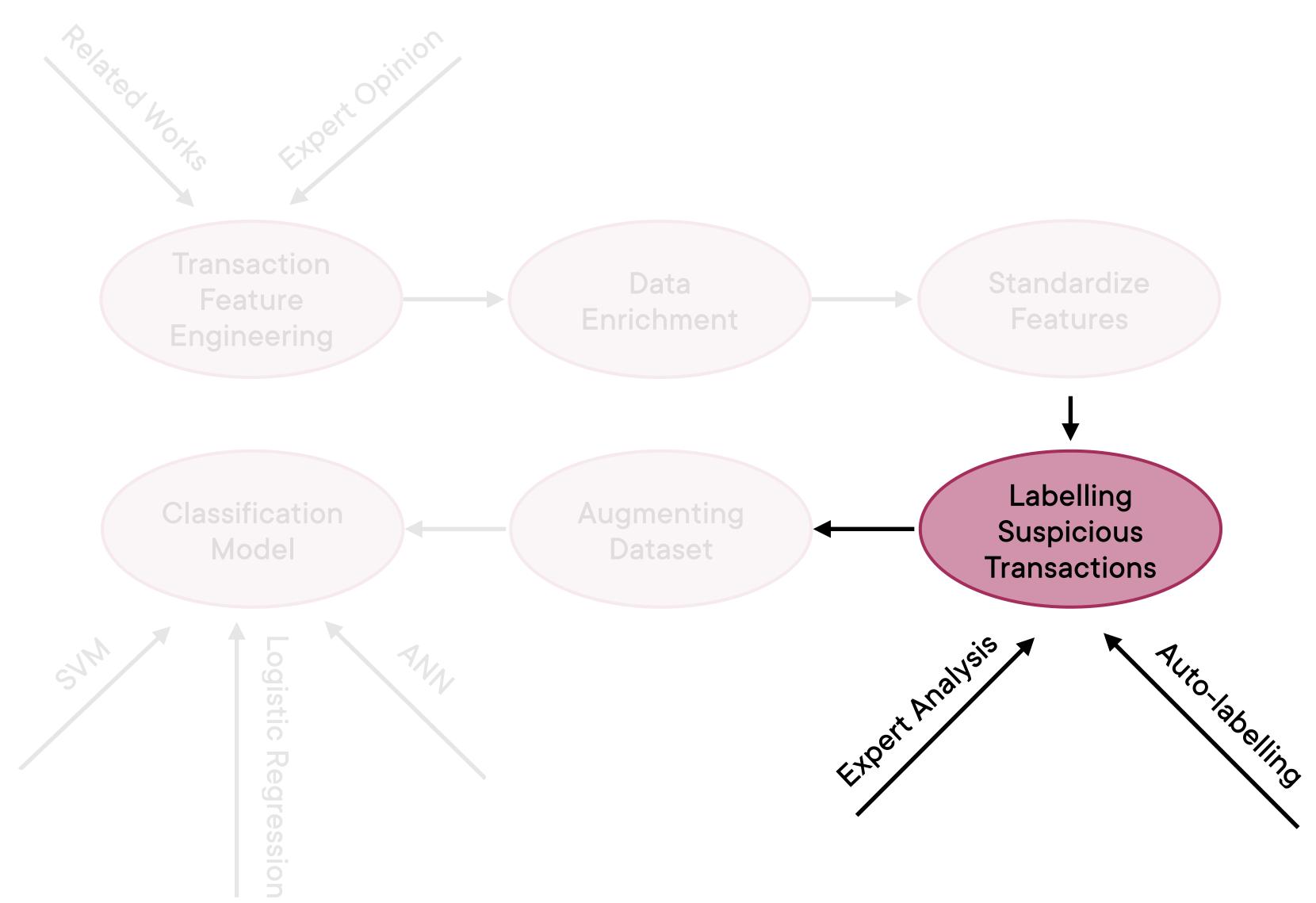
Converting Raw Data to Curated Data



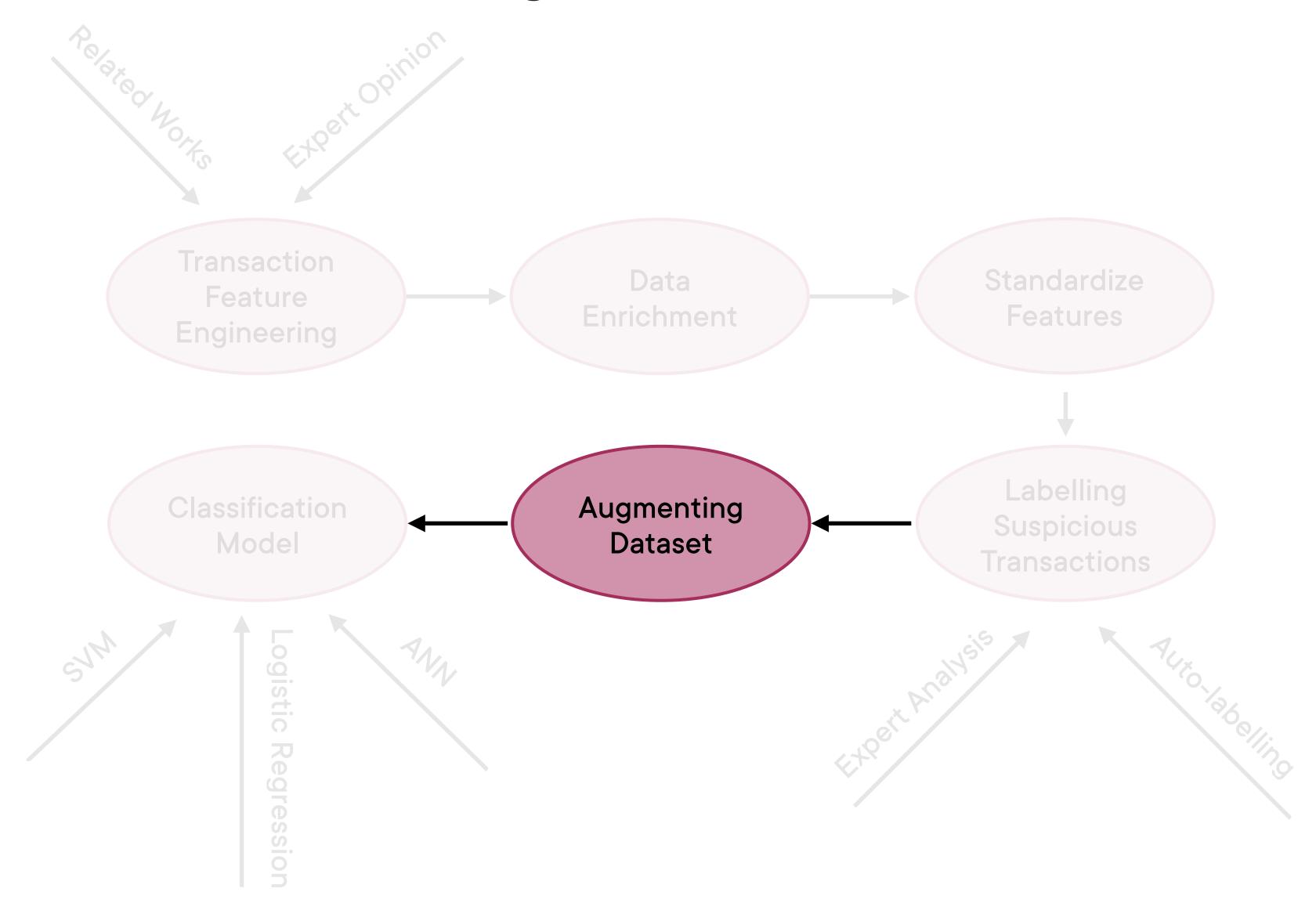
Convert Numeric Features to Same Scale



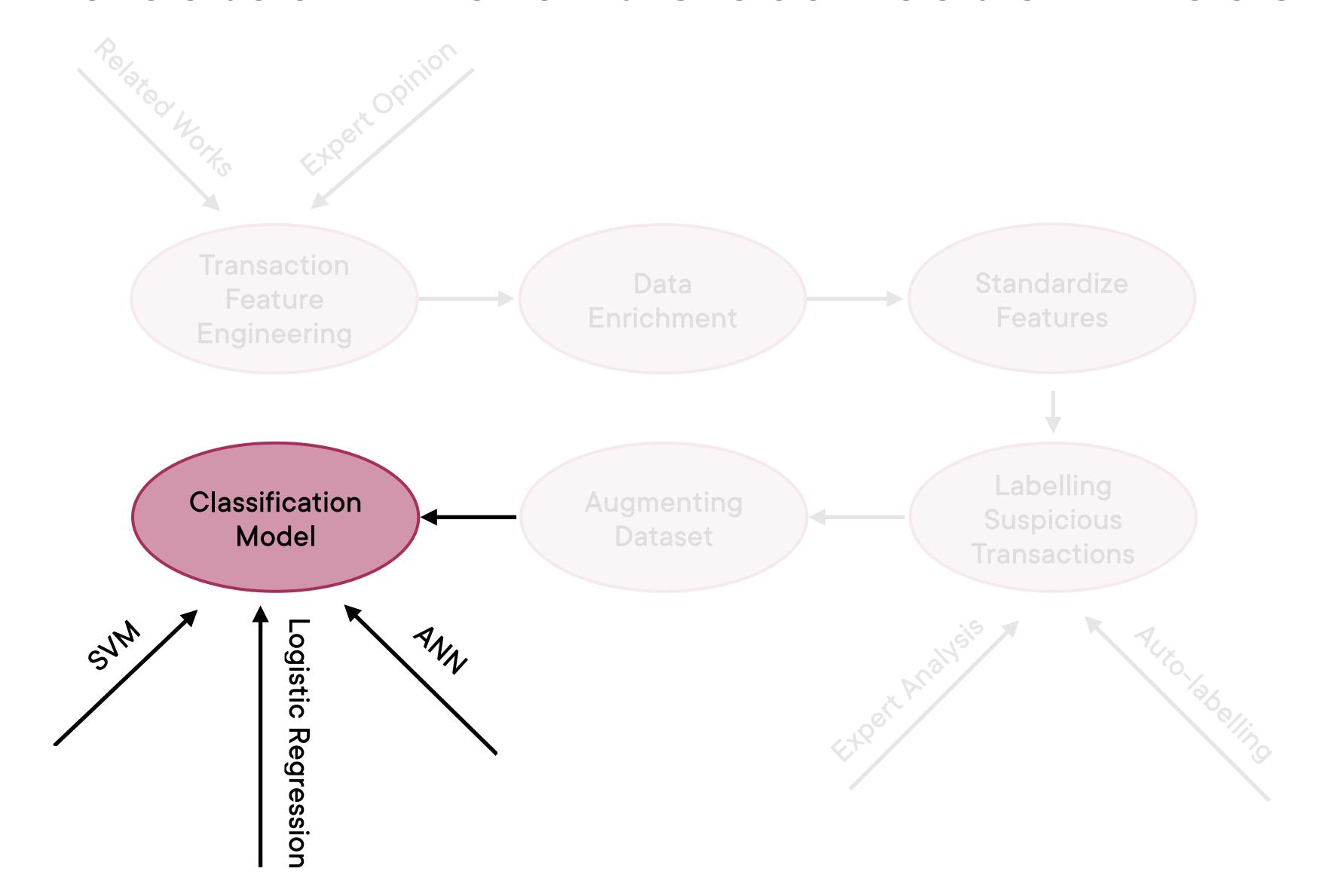
Experts + Snorkel



Balancing Skewed Dataset



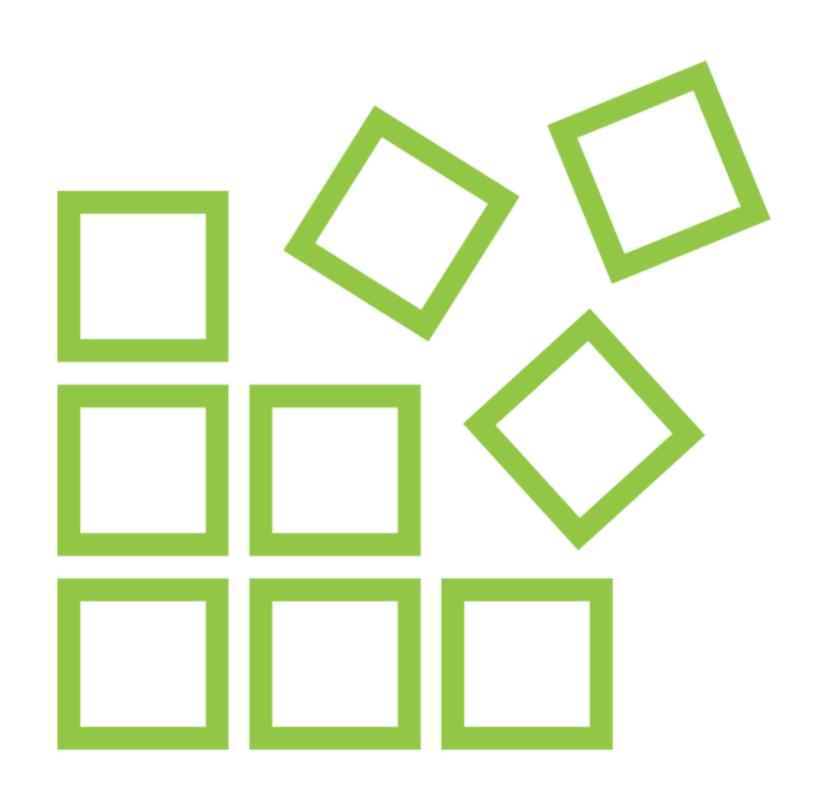
Evaluated Different Classification Models



Classification Model

Classification Method	Accuracy	F1 Score	Recall	Precision
Logistic Regression	0.883	0.874	0.883	0.865
Nearest Neighbors	0.907	0.907	0.908	0.907
Random Forest	0.923	0.911	0.919	0.903
Neural Network	0.924	0.917	0.910	0.924
Naive Bayes	0.908	0.889	0.871	0.908
Multinomial NB	0.706	0.776	0.861	0.706

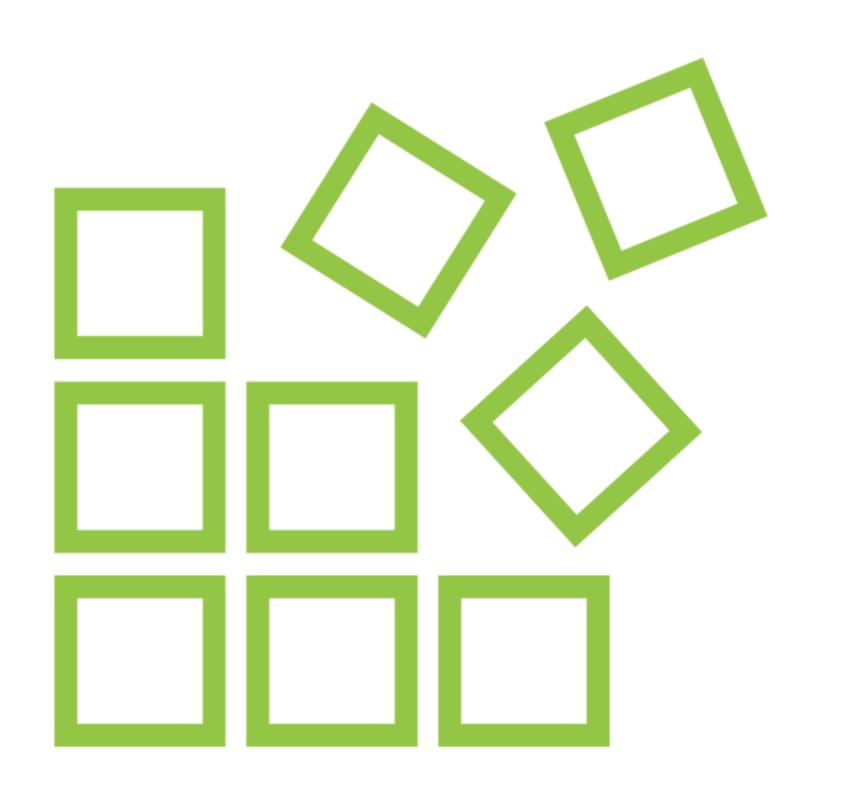
Anomaly Detection



Non-suspicious transactions as training data (no suspicious transactions)

Computed average and standard deviation for transaction features in training data

Anomaly Detection



Combination of regular and suspicious transactions for validation

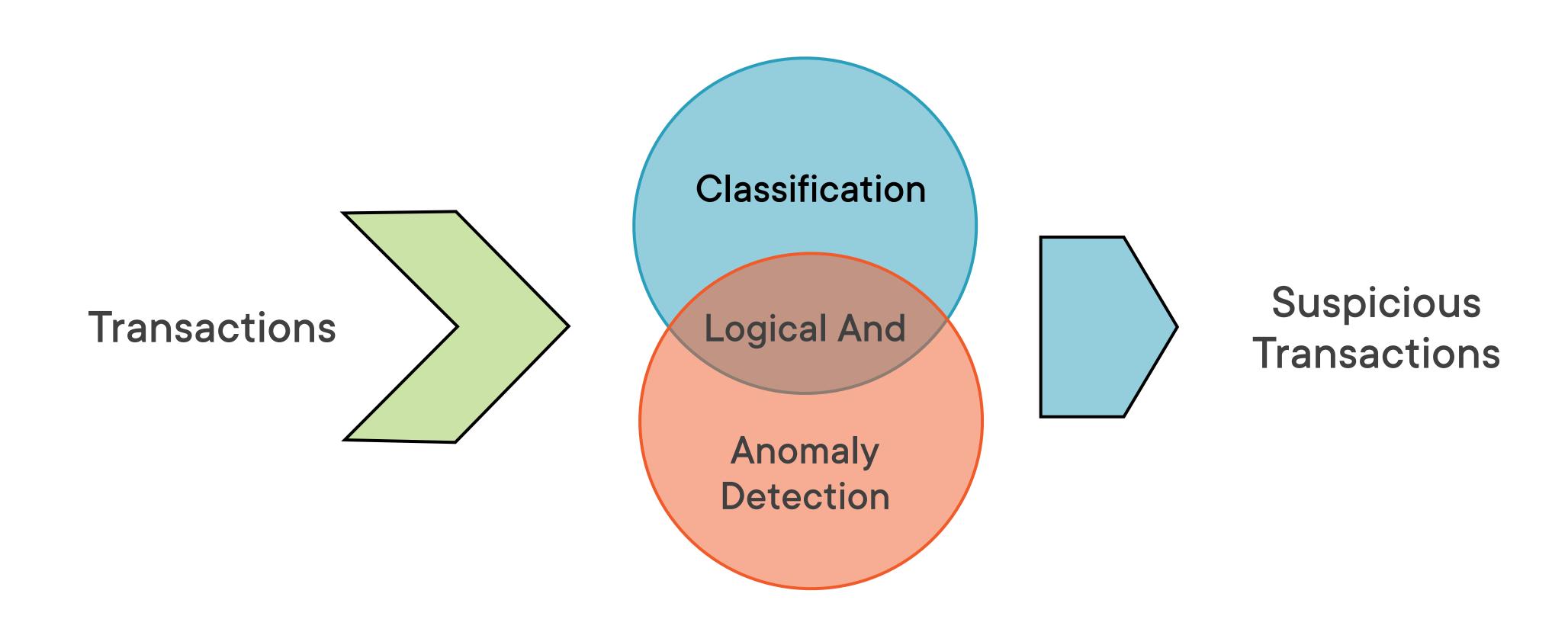
Compute probability for each transaction

Transactions with probability below threshold marked as suspicious

Anomaly Detection

	Result
Accuracy	0.893
Precision	0.904
Recall	0.912
F-1 Score	0.907

Logical AND to Improve Accuracy and Minimize False Positives



Intelligent Hybrid Pipeline

	Result
Accuracy	0.951
Precision	0.939
Recall	0.899
F-1 Score	0.919

Summary

Case Study: Artificial Intelligence Enabled Financial Crime Detection

Up Next:
Applying Machine Learning
Techniques to Financial Data