Ekata Data & You

How Global Buy Now, Pay Later Companies Optimized Customer Experience While Blocking Fraud

Paul-Christian Stoy,
Field Data Scientist

EKATA mastercard

About the moderator

Alan Moss is currently **Managing Director for Western Europe at Newland Payment Technology**, a top international supplier of secure payment devices and associated infrastructure.

Alan has over **20 years' experience in the electronic payments business,** working with industry leaders such as Hypercom, Miura, Thales and Verifone, in a variety of roles from business development and product marketing to global relationship management. Alan also worked in international sales for De La Rue's security holographics and security print divisions.

Prior to working for Newland, Alan was **VP of Marketing at Miura Systems,** a pioneer in mobile acceptance solutions. During his time at Verifone, Alan was also a **board member and Chairman of the General Assembly of Nexo**, a leading pan-European standardization initiative promoting the interoperability of card payments.

About the speaker

Paul-Christian Stoy | ***Field Data Scientist***

Paul is a Field Data Scientist at the EMEA office of Ekata.
In his role, he is working with Ekata's customers to reduce fraud while minimizing customer friction at account sign-up and during the transaction flow. His projects cover a range of industries, fraud types and detection systems.

Before joining Ekata, Paul worked in different analyst and consultant roles. He holds degrees in data science and business administration.

Ekata, a Mastercard company, currently has over 2,000 customers globally, including companies like Alipay, Equifax, Klarna, and Microsoft.

Contact: paulchristian.stoy@ekata.com

Trusted by Global Enterprise Organizations

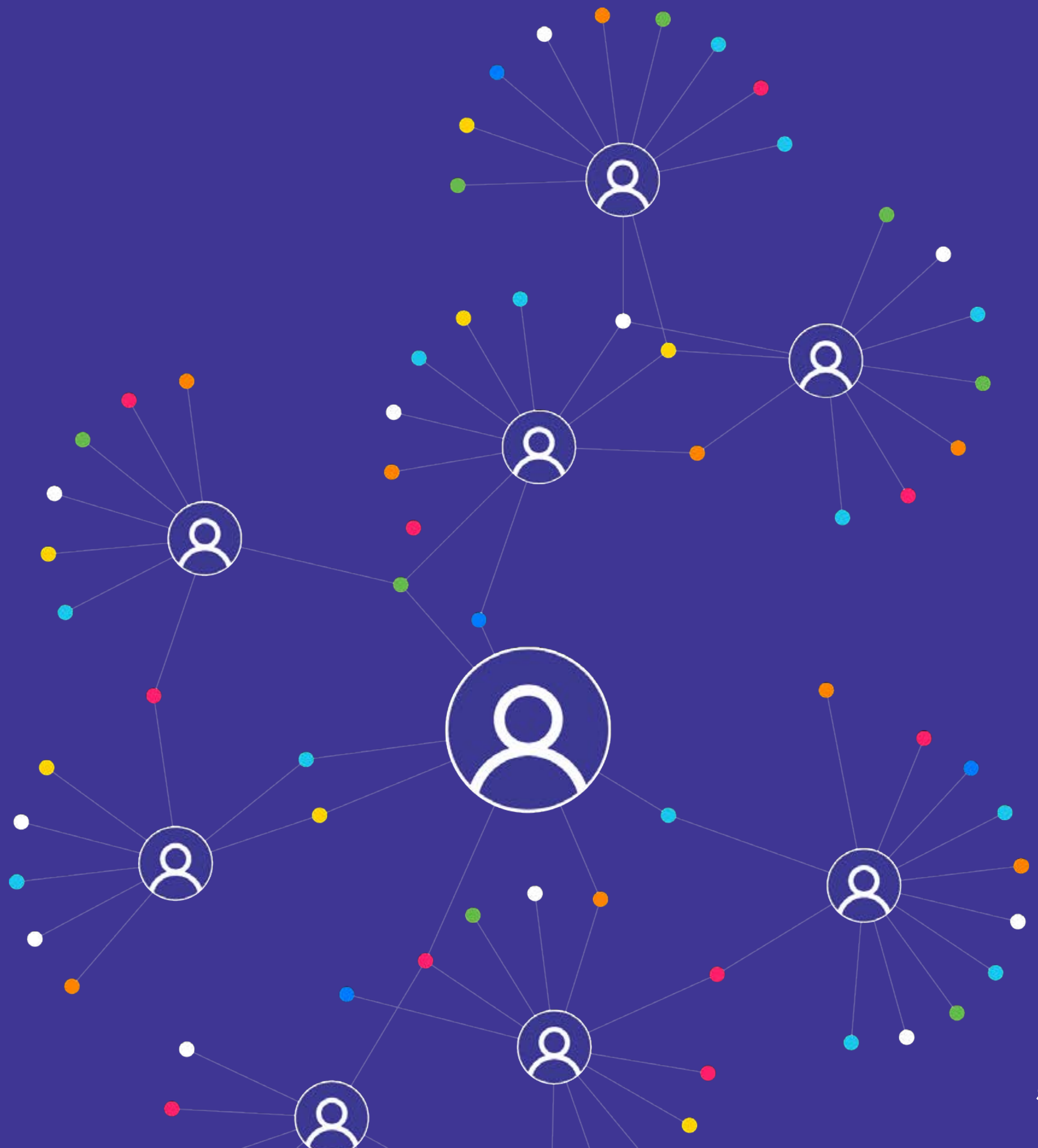
Online Lending	Global Payments	Marketplaces	Travel	eCommerce	Fashion
Goldman Sachs	checkout.com	lyft	Expedia	amazon	adidas
Klarna.	stripe	airbnb	Booking.com		FARFETCH
DISCOVER	Square	match	KLM	Microsoft	YOOX NET-A-PORTER GROUP
affirm	AMERICAN EXPRESS	POSTMATES	Emirates	IKEA	MYTHERESA
AVANT	Alipay	Nextdoor	FINNAIR	NESPRESSO.	THEHUTGROUP

Partner and Resellers

Kount, CyberSource, adyen, sift, SIGNIFYD, Nethone, FORTER

Accertify (an American Express company), experian, DemystData, trunarrative, simility, riskified, ACI UNIVERSAL PAYMENTS

Digital Account Opening Challenges



Solving Digital Onboarding Challenges

Streamline Account Opening Processes

- Meet expectations of good customers by removing friction
- Streamline KYC and reduce manual review effort

Mitigate Fraud

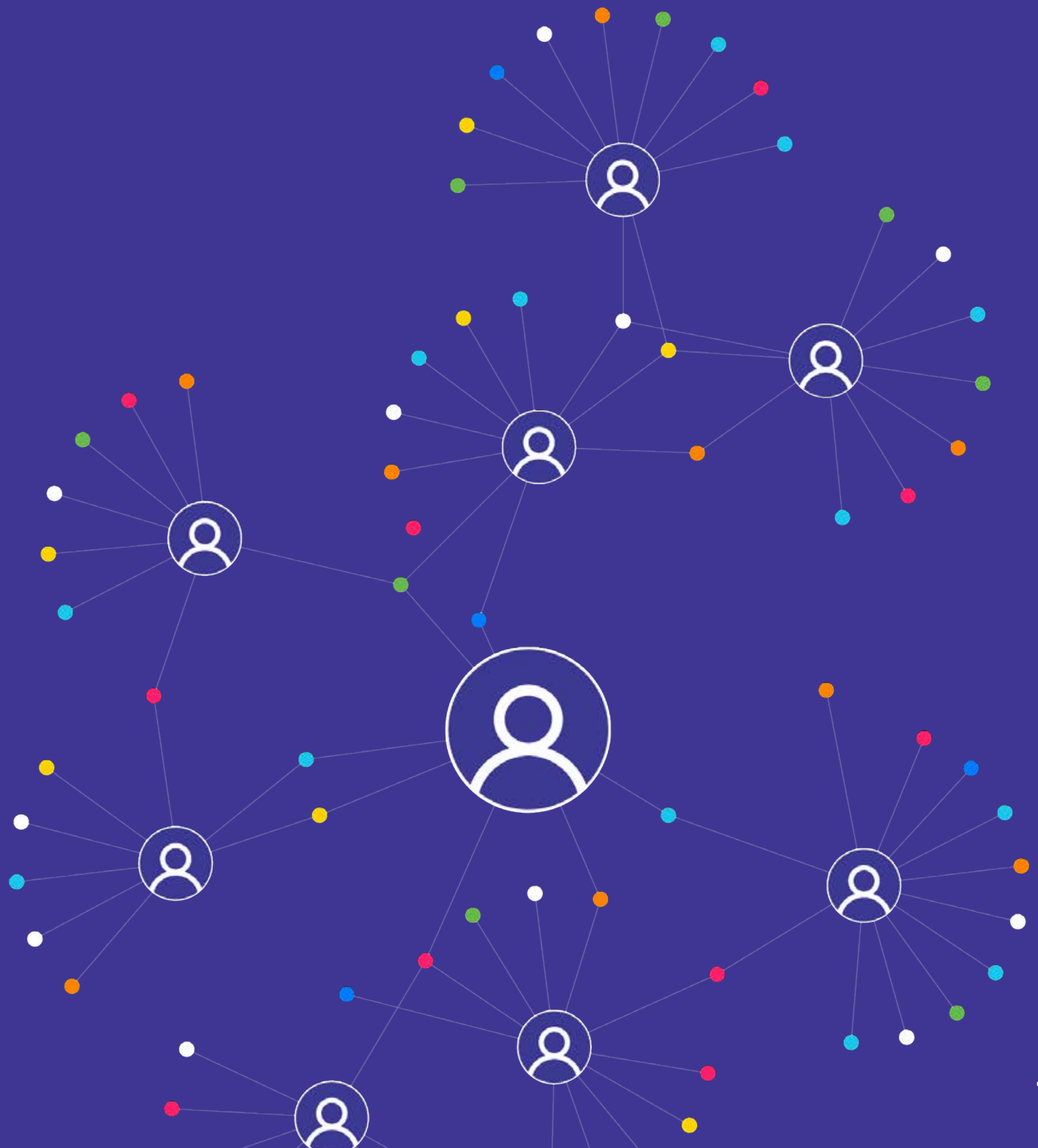
- Capture compromised / synthetic identities
- Avoid never-pay fraud before losses

Overcome cold-start and thin-file customer issues

- Enrich customer information with predictive fraud risk signals
- Avoid unnecessary step-up authentication

Enable near real-time decision-making

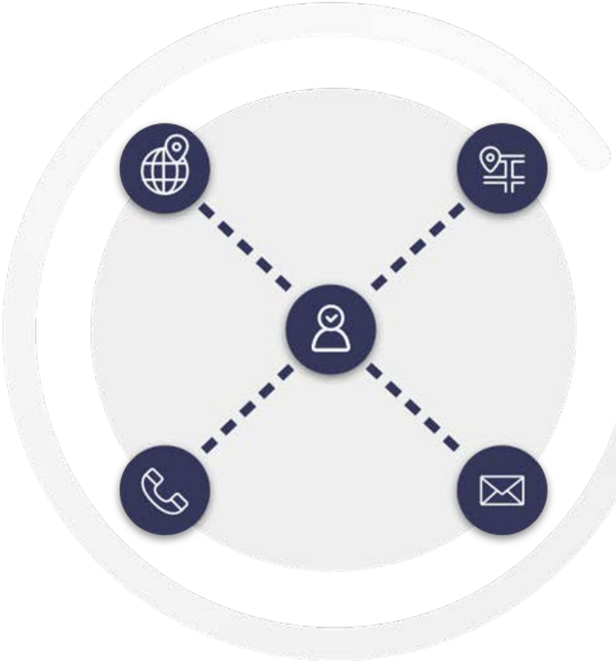
How Ekata Helps With Passive Authentication



The Ekata Identity Engine

Identity Graph

Database that validates digital identity elements and how they are linked

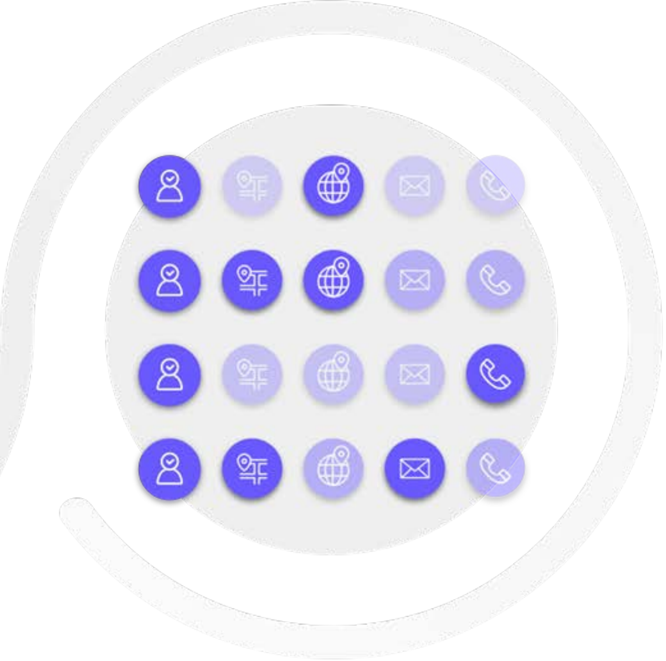


7B+
entities

1B+
identities

Identity Network

Anonymized database that surfaces patterns of how hashed identity elements are being used online



16B+
identity elements

40M
elements added per day

EKATA mastercard

Account Opening API | Responses

Identity Risk Score
Output between 0 to 500

Identity Network Score
Output between 0 to 1

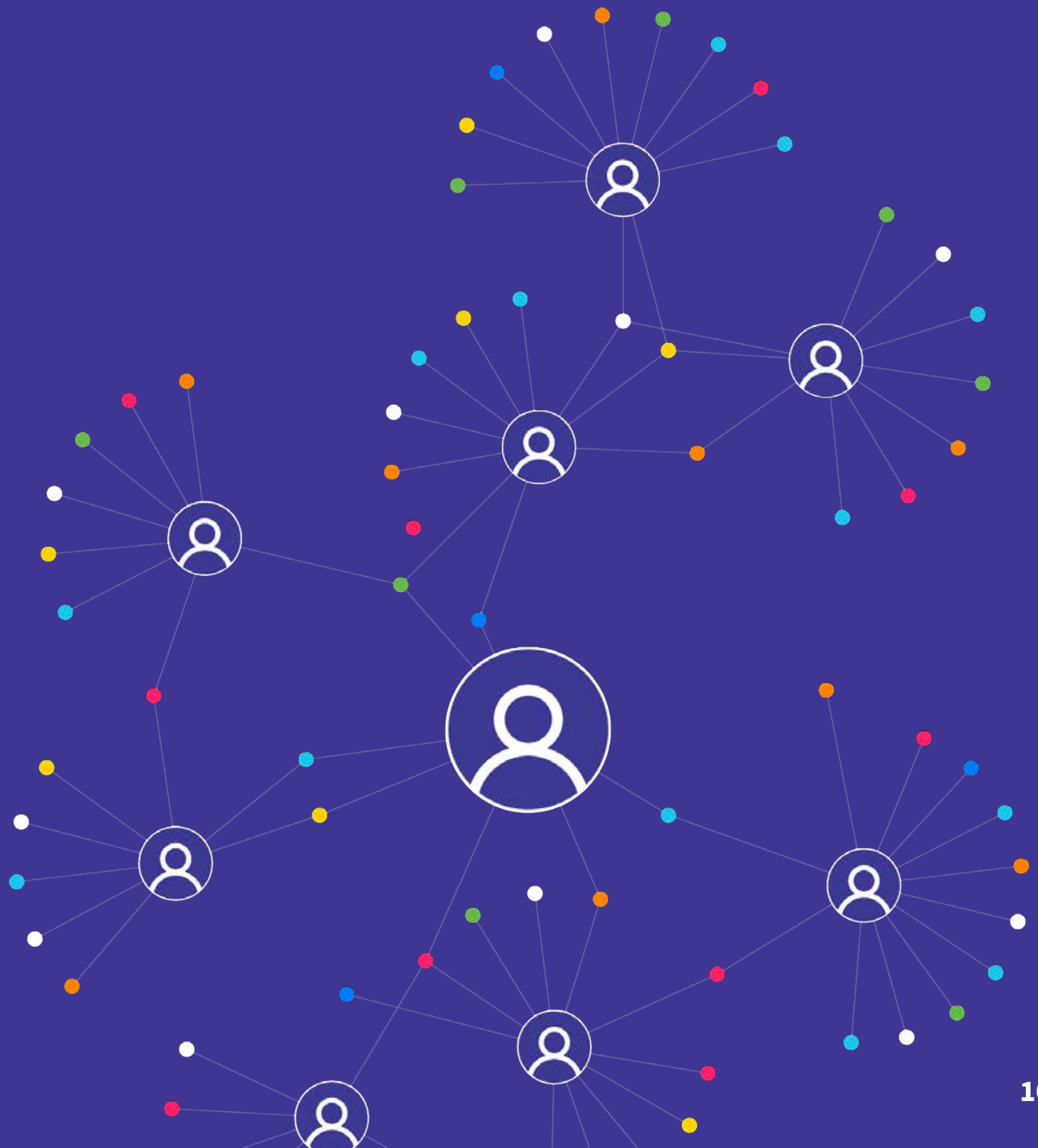
Phone
- Match to name
- Match to address
- Is valid
- Line type
- Carrier
- Country code
- Last seen days
- Linked to email days

Address
- Match to name
- Is valid

Email
- Match to name
- Is valid
- First seen days
- Domain creation date
- Linked to phone days

IP Address
- IP risk flag & score
- Last seen days
- Distance from address
- Distance from phone
- Country code
- Subdivision

Case Study



Proof of Concept - Stages

1 Define Joint Test Plan

2 Workflow mapping

3 Point-in-time API Batch Run

4 Exploratory Data Analysis

5 Create Recommendations

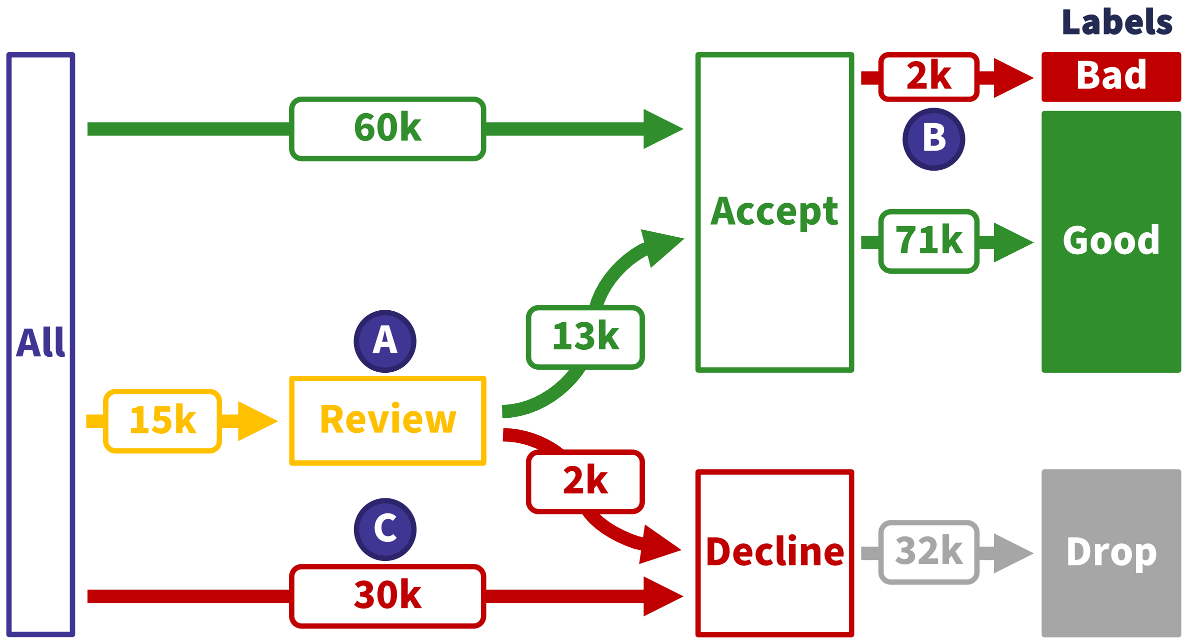
6 Present Results

Define test type and structure to accomplish the goals

Obtain Ekata API responses for historical customer data and identify fraud patterns based on outcome labels

Provide recommendations specific to the customer's fraud system (e.g., rule- or ML-based) on how to accomplish their set goals

Account Opening Workflow
Customer Problem Definition



Identified problems:

A. **14% review rate with 87% acceptance**

B. **2.7% accepted fraud rate**

C. **29% reject rate**

EKATA mastercard

Ekata feature EDA
Streamlining the analysis using feature importance

Create Training and Testing Datasets

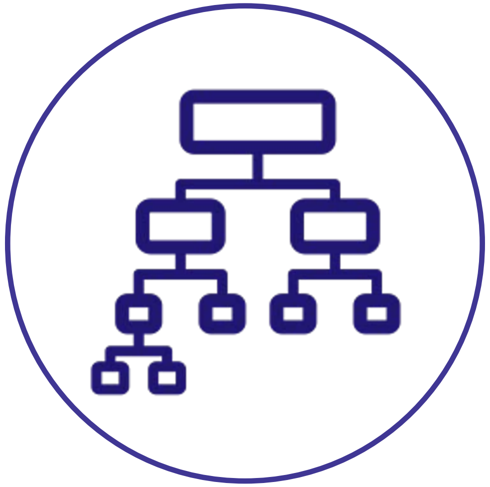
Build model

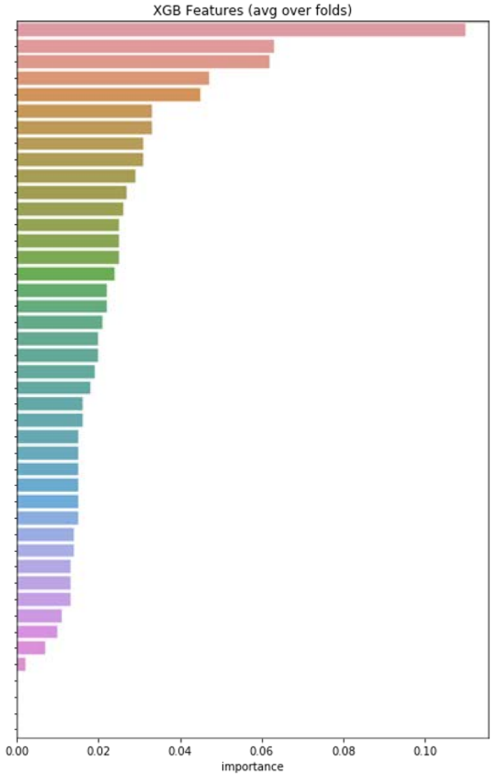
Obtain feature importance

Ekata point-in-time API responses for historical account openings

+

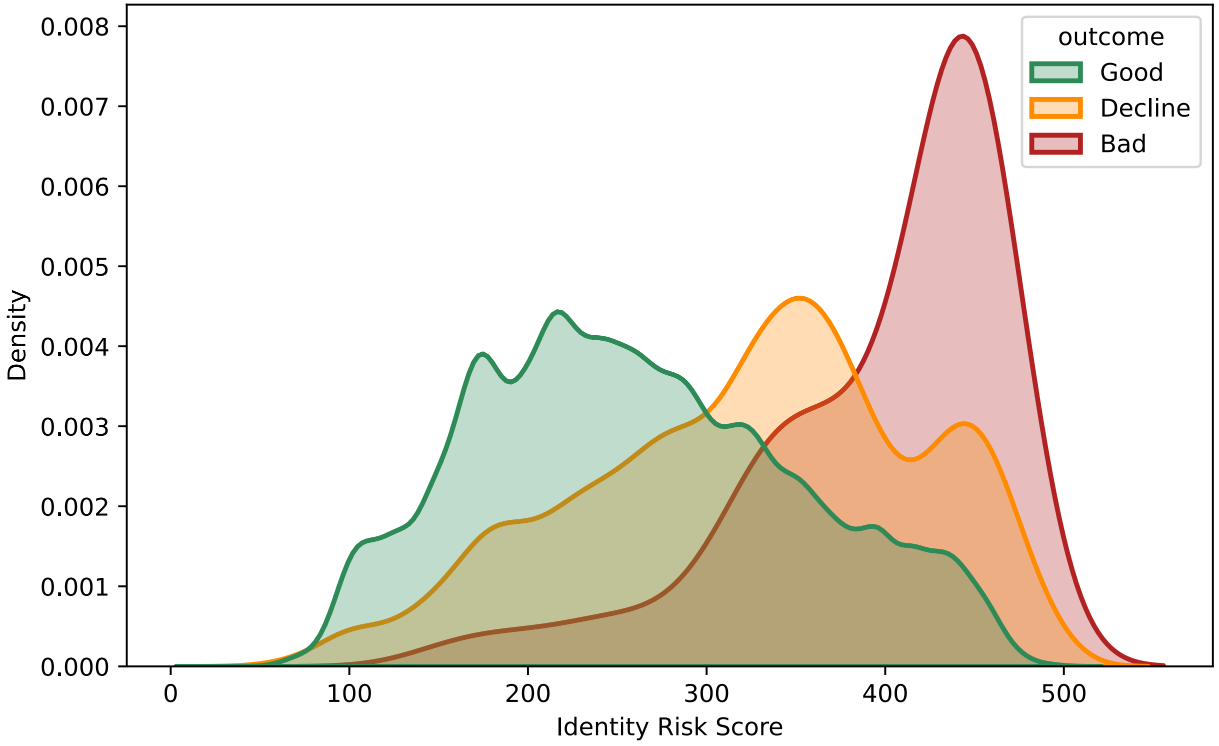
Outcome Labels (Fraud vs. No fraud)





Ekata feature EDA
ML Scores: Identity Risk Score

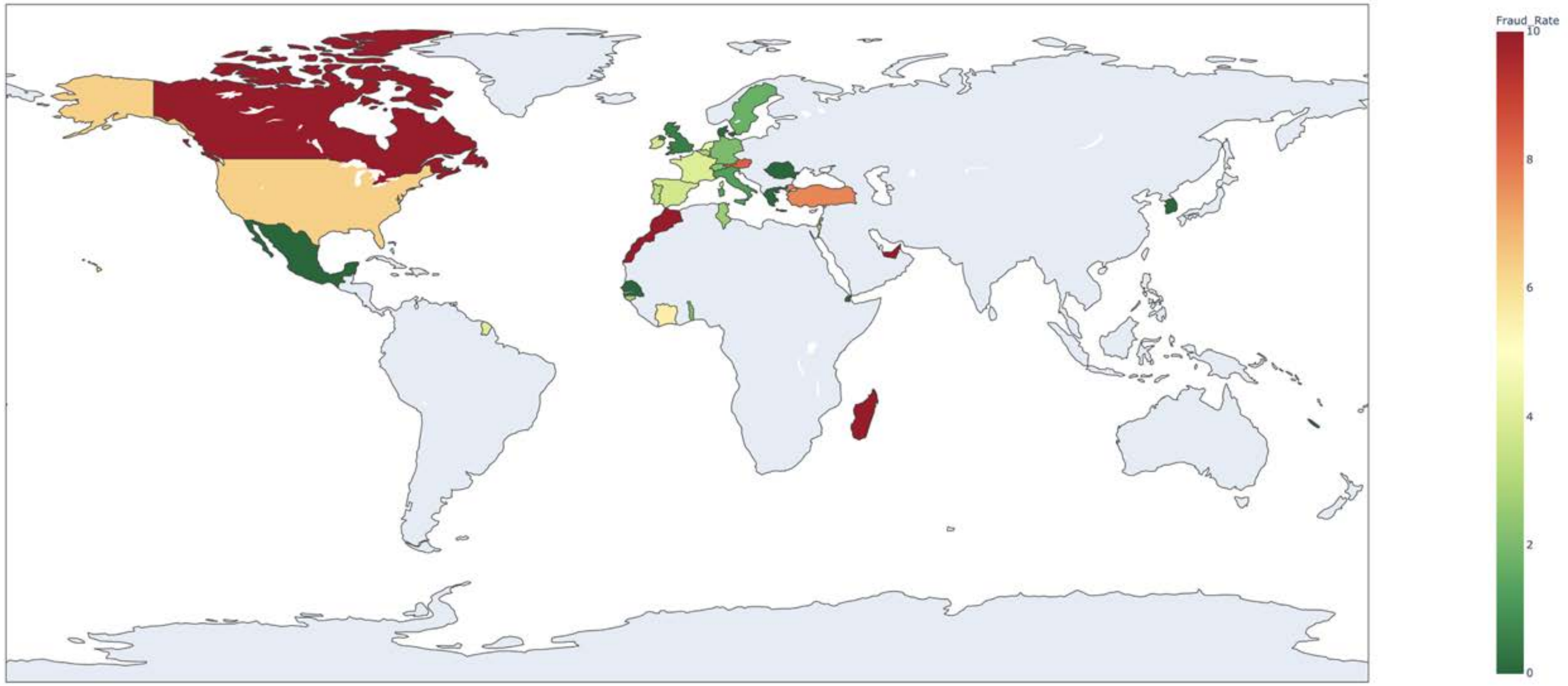
- 0-500 scale where low scores represent low risk, and high scores represent high risk.
- Clear separation between good and bad customers
- ‘Mixed’ rejected population indicates false positives
- Risk score demonstrates Ekata’s probabilistic approach to tackling fraud



Ekata feature EDA
PII Metadata: IP Geolocation Country

- Identify origin-specific fraud patterns
- Strong basis for feature engineering
  - E.g., IP country equals billing country
- Not to be used a sole basis for decision-making

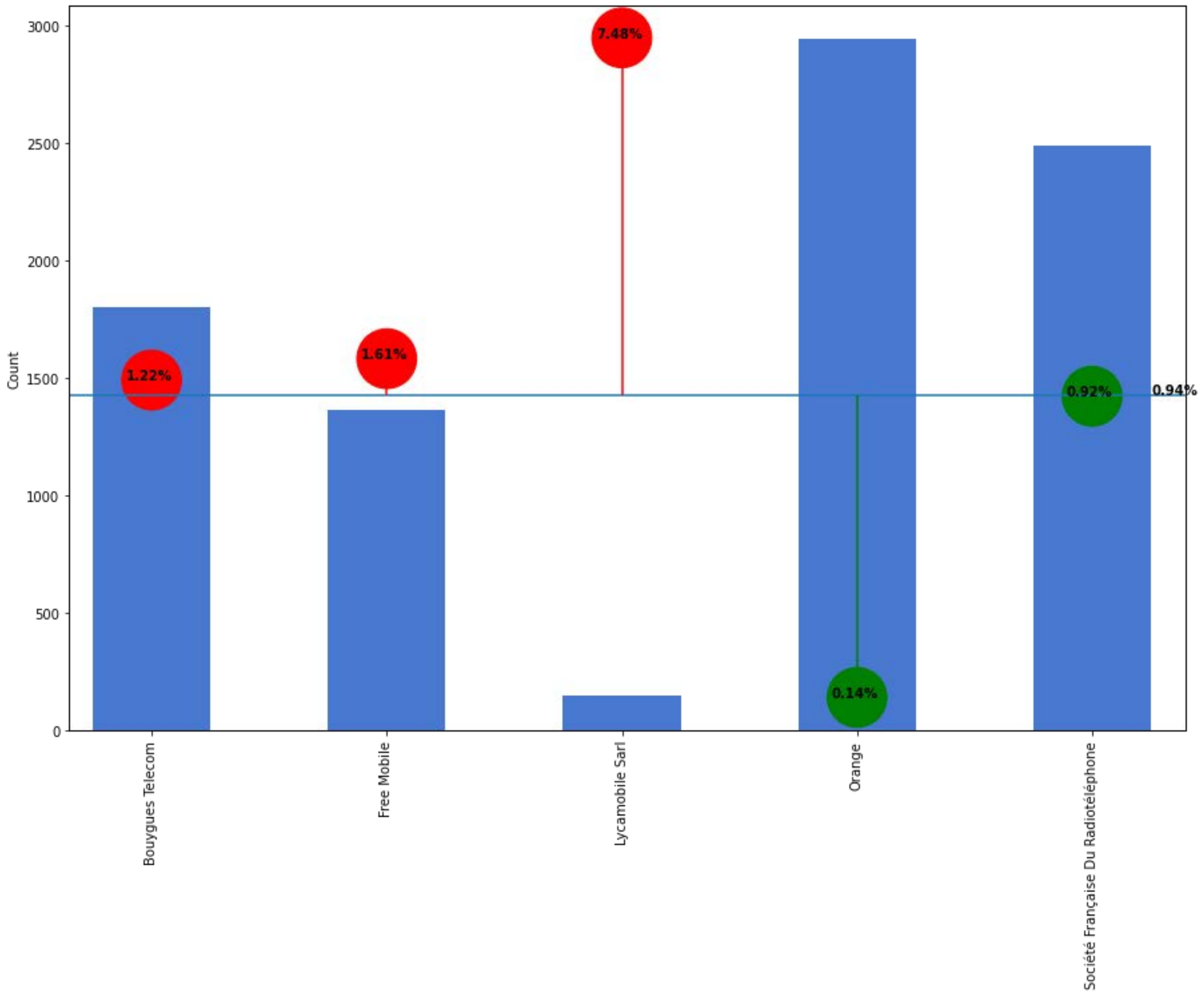
Fraud rate by country



Ekata feature EDA
PII Metadata: Phone Carrier

- Returns the carrier of the phone provided in the transaction
- Distinct differences seen in fraud rates based on the phone carrier

Subset FR data

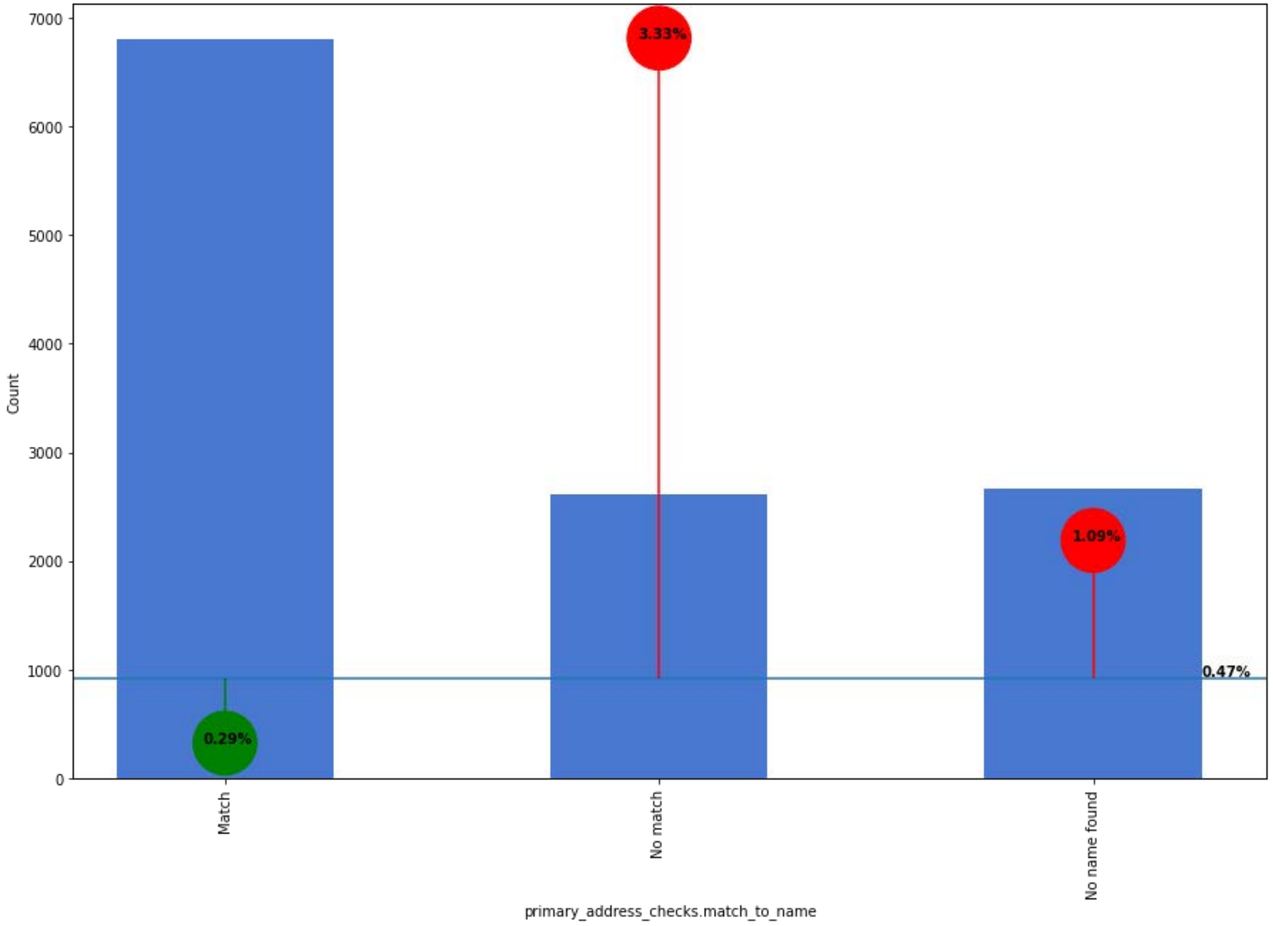


Ekata feature EDA
Matching: Address to Name

- Returns a match, no match, or not found based on whether we are able to match the address to the name on the transaction.

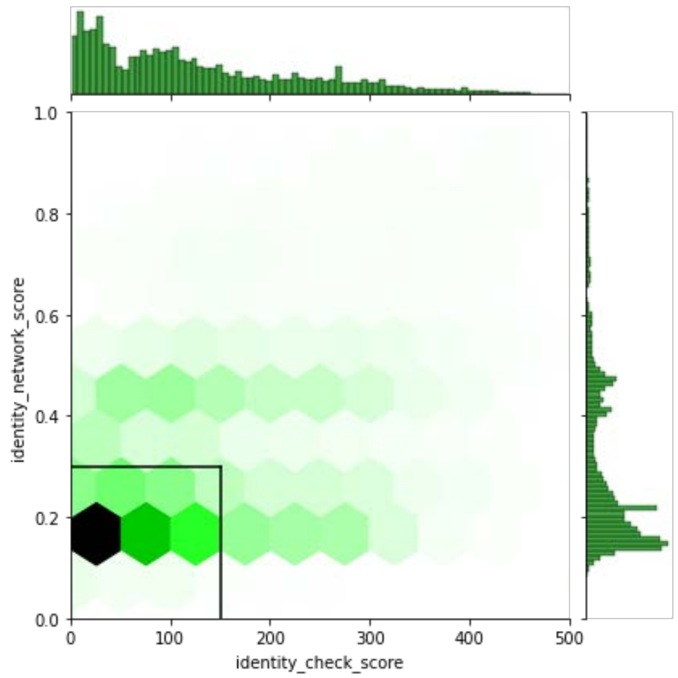
- When the address and the name match, the fraud rate is 10x lower compared to no match.

Subset UK data

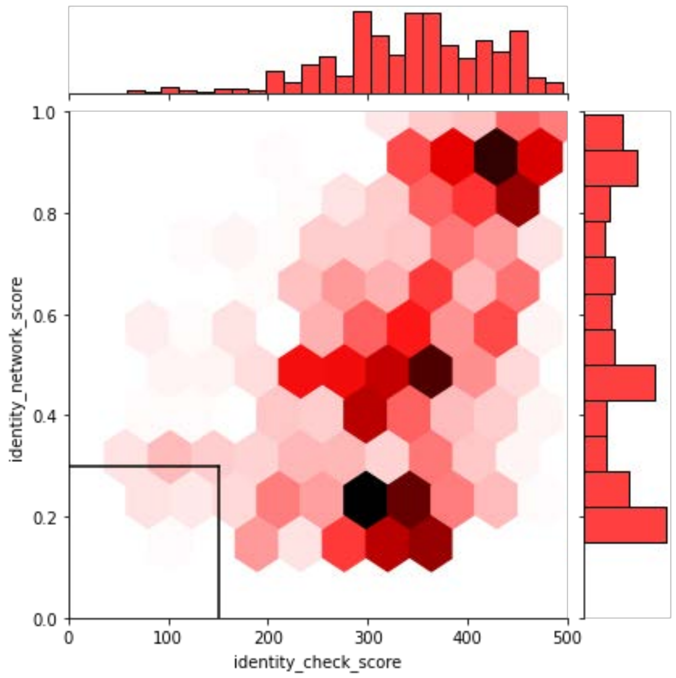


Combining Signals
EDA to identify potential false positives

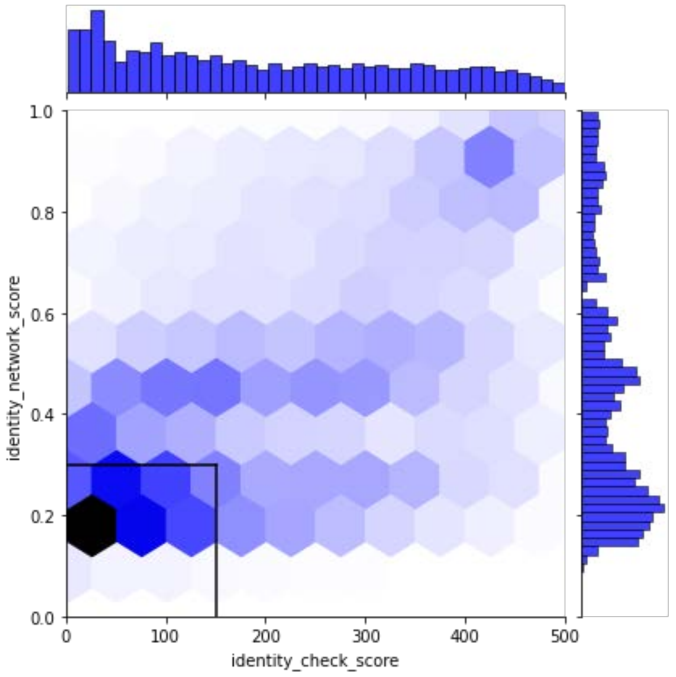
Good Customers



Bad Customers



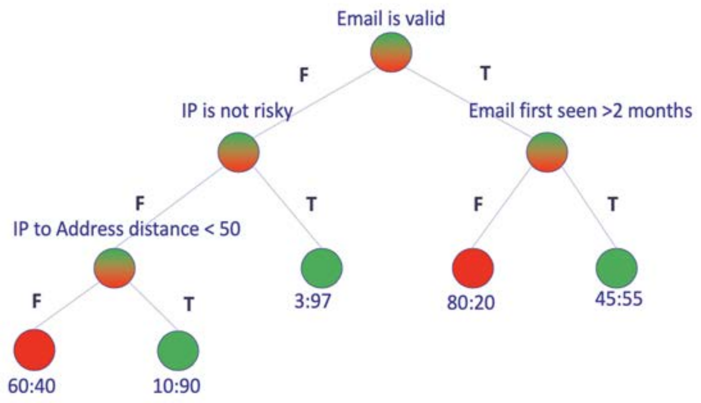
Rejected Customers



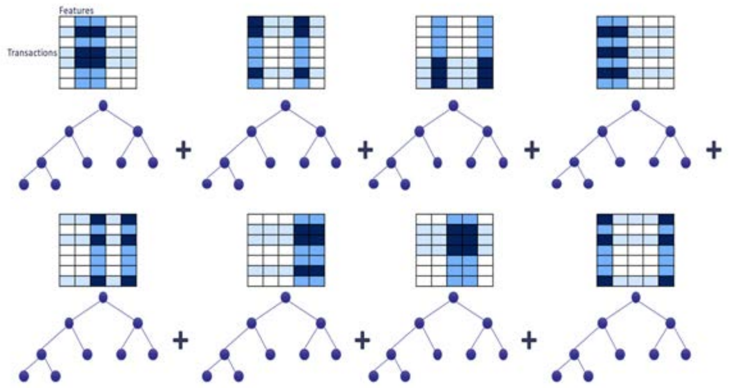
99% Accurate against confirmed bad customers

Creating Rules
Use of ML to find optimal features combinations

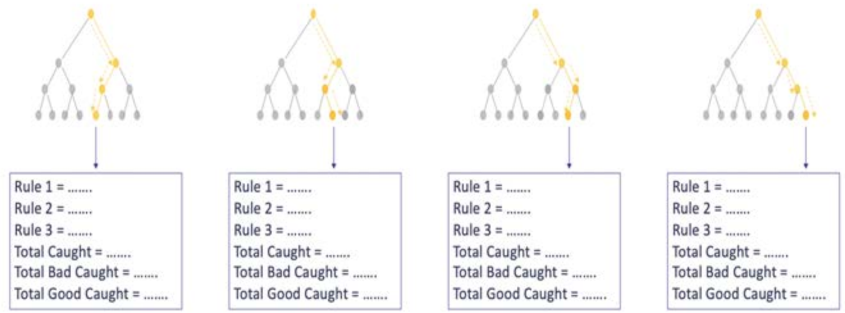
1. Decision trees are made of logical gates



2. Build many trees with different subsets of features and records

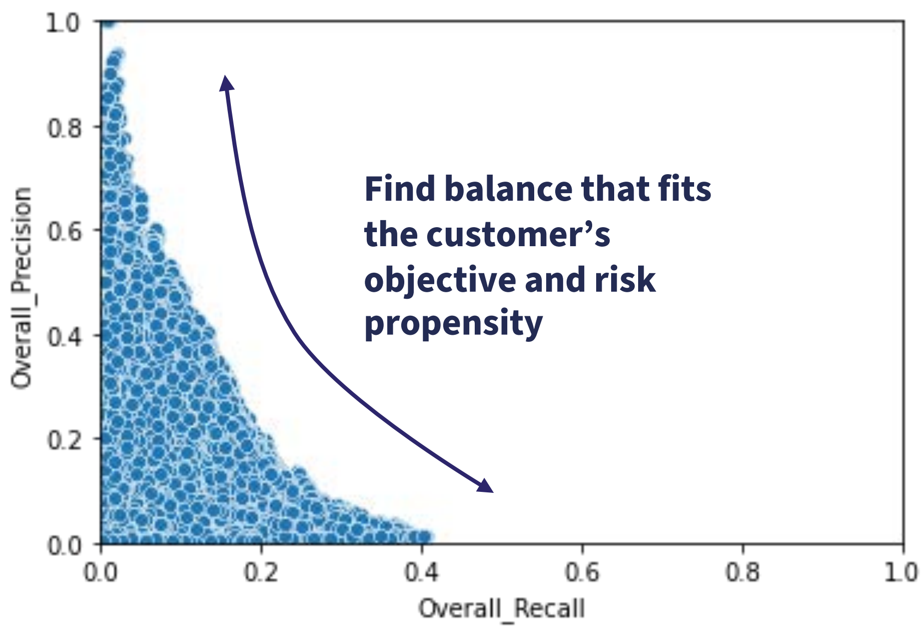


3. Extract the rules from each logical gate for every tree and assess overall performance



Creating Rules
Rule selection based on customer objectives

Typical precision-recall tradeoff in rule-building



Find the optimal combination of rules (potentially with different foci)

1. Good-focused rules:

- **Reject to Review / Accept**
- **Review to Accept**

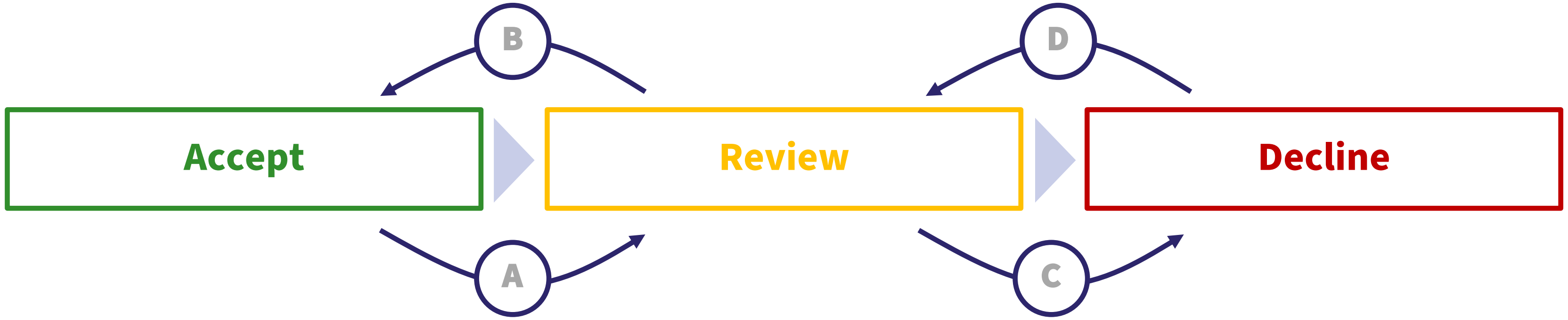
→ **Reduce customer friction, increase acceptance**

2. Bad-focused rules:

- **Accept to Review / Reject**
- **Review to Reject**

→ **Reduce fraud**

Customer Impact - Overview



A — 3 x Accept Bad-focused Rules (34% recall at 75% precision)

B — 2 x Review Good-focused Rules (19% recall at 99% precision)

C — 2 x Review Bad-focused Rules (11% recall at 98% precision)

D — 1 x Decline Good-focused Rules (5% recall at 90% precision)

Key Take-Aways

Passive identification using probabilistic fraud risk signals:

- Clear problem definition + success metrics
- Comprehensive EDA: Understand the ‘why’ behind the signals
- Use of Machine Learning of optimize the recognition of fraud patterns

Questions?