ASB
ONE STEP AHEAD

Leveraging Analytics to Solve Business Problems

Aisling Gu, Data scientist

Content

- Introduction
- Analytics
    - Traditional analytics
    - Analytic with generative AI
- Bank quiz!
- Case study

Tools & platform

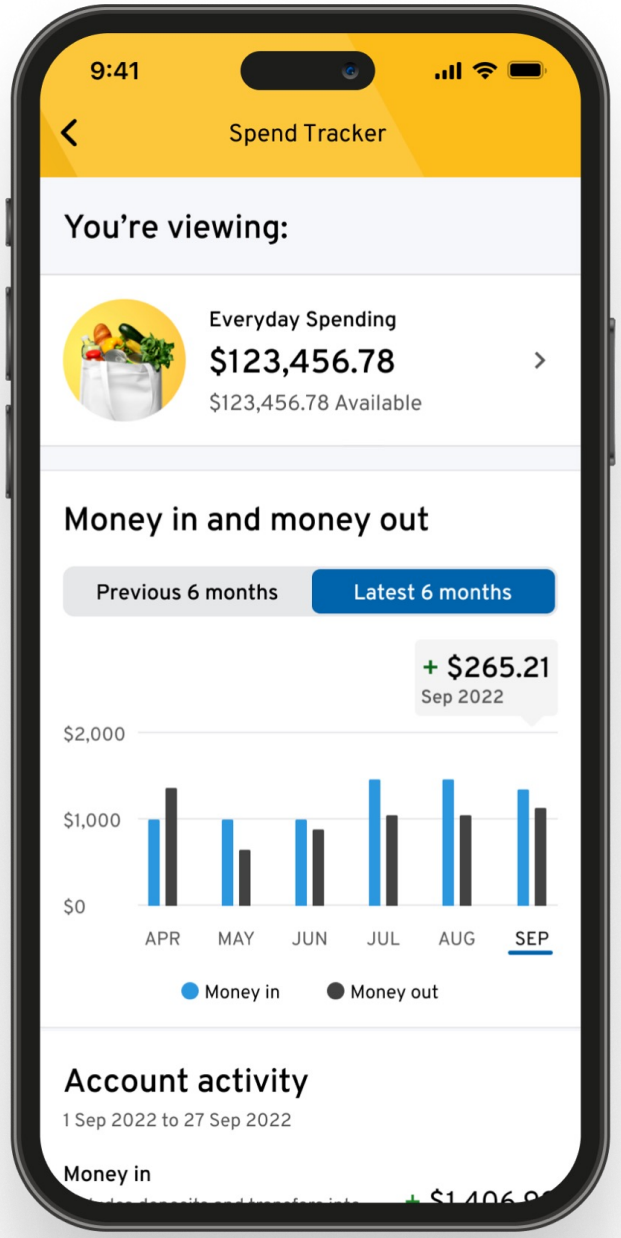
- More tooling to come

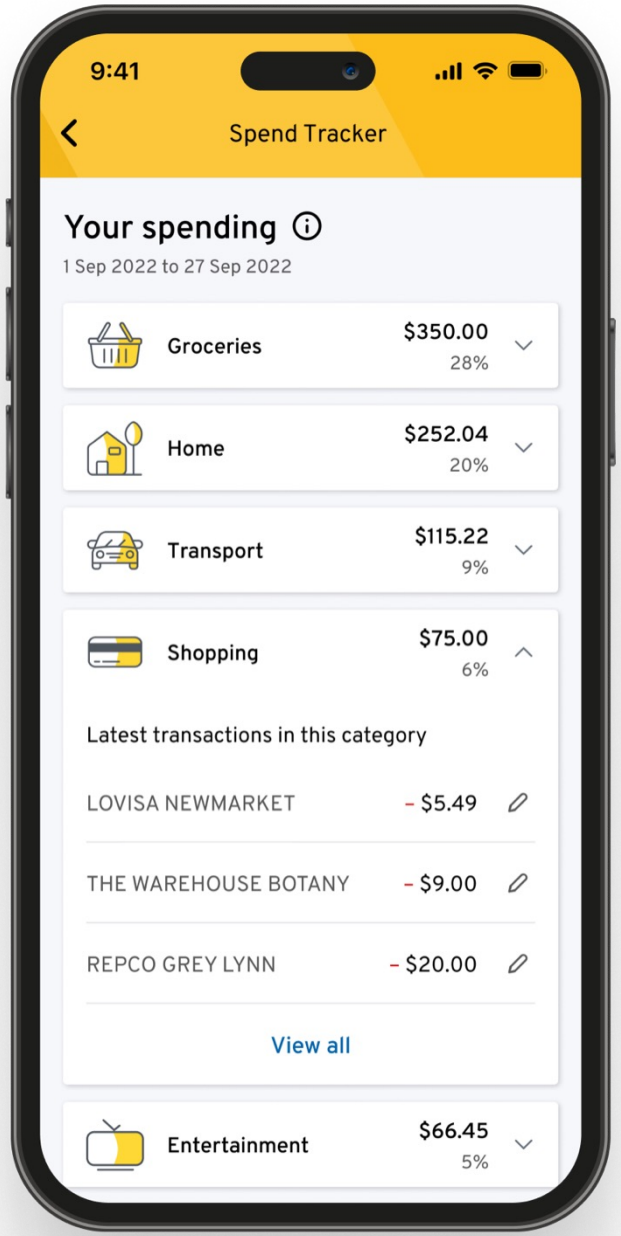
Traditional Analytics Spend Tracker

Spend Tracker

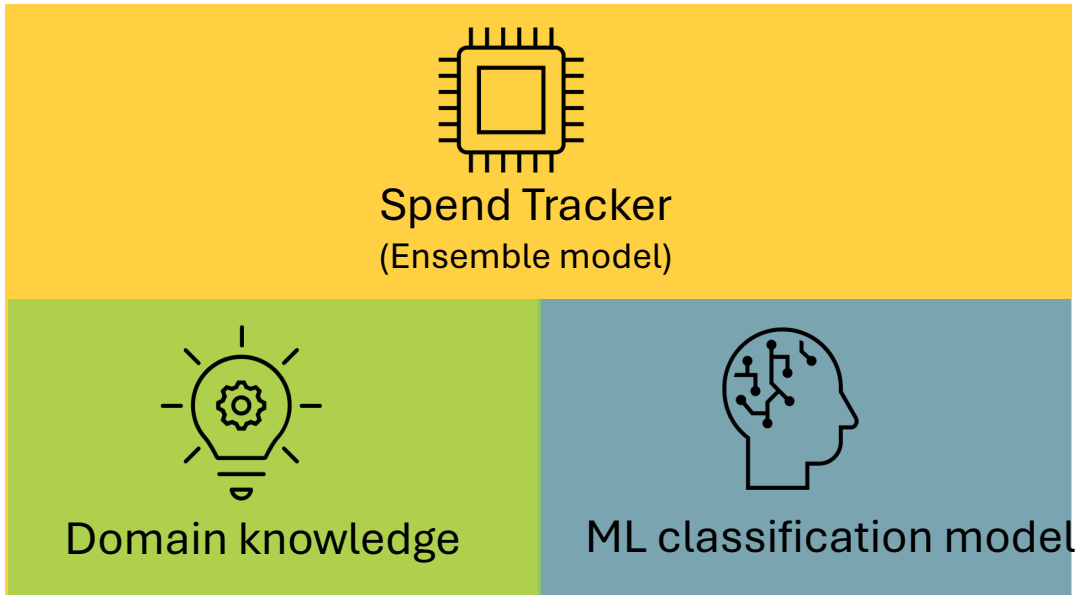
ASB Financial Wellbeing Tool

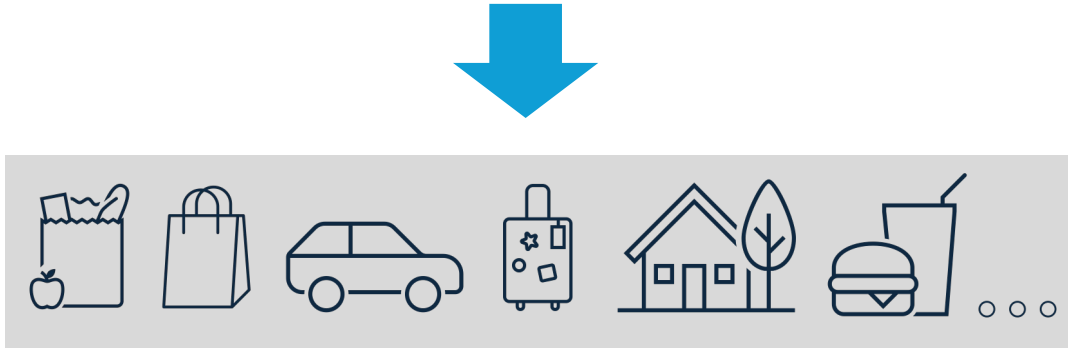
- SpendTracker experience powered by our model (on Databricks!)
- Classification up to 18 different categories





Spend Tracker Model



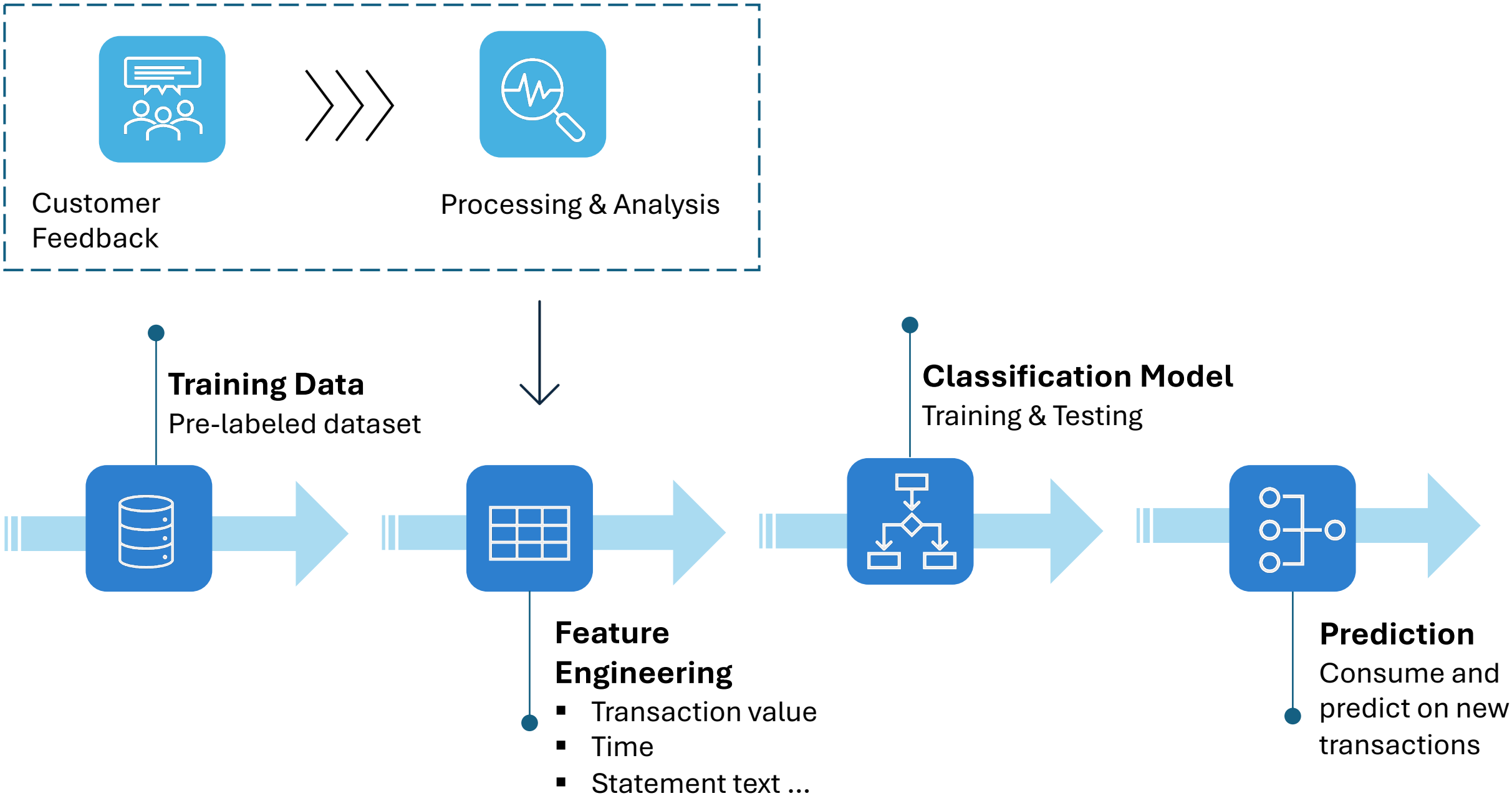


```
Merchant Category Code
5411 Grocery Stores and Supermarkets

Time: 05/02/2022 16:00

Statement Text:
COUNTDOWN LYNFIELDAUCKLAND

Value: $75.00
```


Customer Feedback
Processing & Analysis
Training Data
Pre-labeled dataset
Feature Engineering
Transaction value
Time
Statement text ...
Classification Model
Training & Testing
Prediction
Consume and predict on new transactions

Analytics with generative AI
Abusive Transaction

Industry Response

Newshub.

24 February 2023

HOME NEW ZEALAND WORLD POLITICS SPORT ENTERTAINMENT

LIVESTREAM AM

BANKING

Abusive messages through bank transfers becoming 'increasingly common' - family lawyer

trending tech innovation business security advice

Home / Finance

Westpac has blocked 24,000 abusive messages in payments

Westpac's zero-tolerance tool required 19,000 customers to change the language of their transaction description before payments were processed.

Written by **Aimee Chanthadavong,** Contributor on Sept. 20, 2021

Stuff

business

money

BNZ finds 12,000 abusive online banking transactions over six months

Sarah Robson of RNZ • 07:42, Jan 25 2022

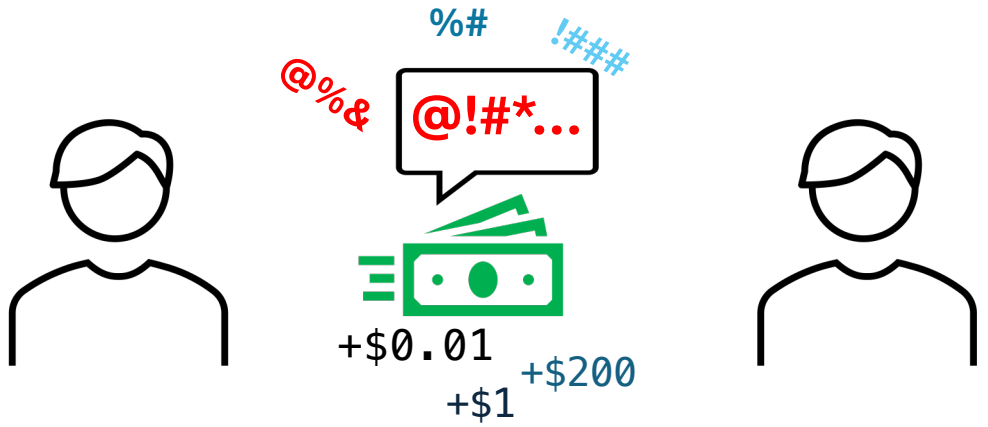
ASB:

Data Science work with Customer Outcome team together to identify these potential abusive transactions

Abusive Transaction

- Transactional abuse is where abusers will use the reference field to send messages while sending money.
- It has been identified an increase in the misuse of payment text fields in financial transactions as a method of criminal communication or abuse, rather than the primary purpose of transferring funds. Instead the transaction text fields are being used with increasing frequency to communicate for the purpose of stalking, harassing and threatening behaviour, or to avoid law enforcement scrutiny.

- Financial indicators
  - Value
  - Volume
  - Relationship
  - Payment Text Fields



A different user case

A lack of offensive or abusive language does not deem a payment message harmless.

Some payment text do not contain overtly threatening language but when accompanied by high volume or low value payments may be harmful.

Sentiment analysis

Positive Neutral Negative

Quiz time!

ASB
ONE STEP AHEAD

Case study
Fraud Detection Challenge

Frauds can be deceptive, so as genuine ones

Fraudulent

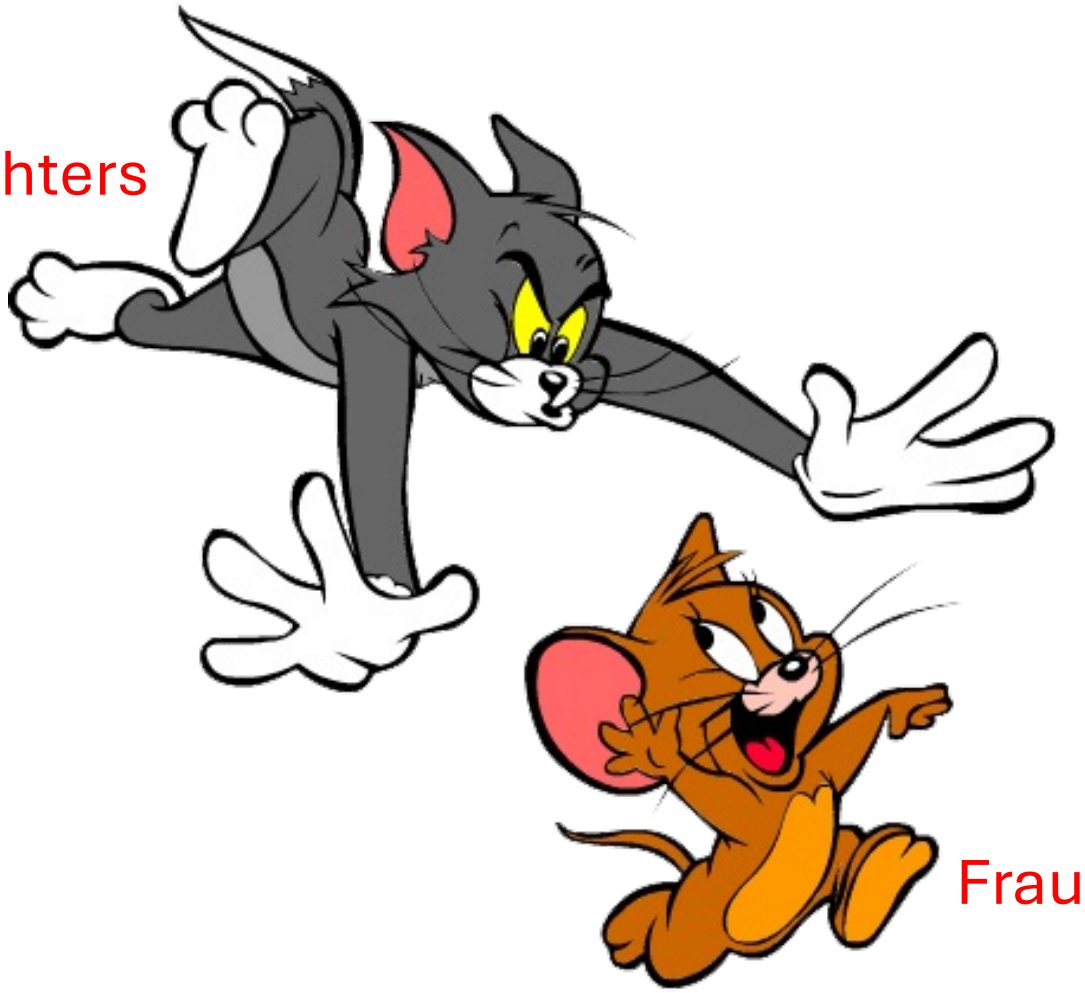
Genuine

Finding needle in the haystack

- Card not present (CNP): **1** fraud in **800** genuine transactions
- Card present (CP): **1** fraud in **30000** genuine card swipes

We are always behind

Fraud Fighters



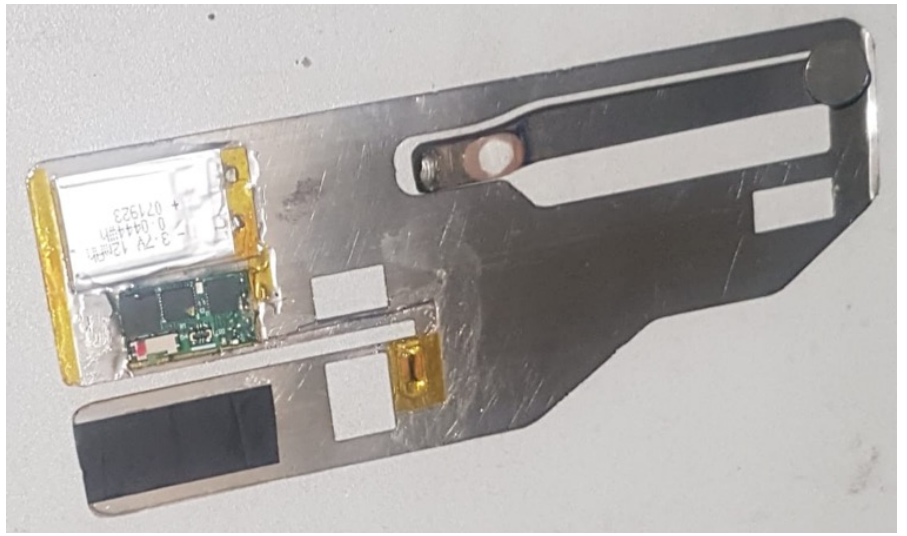
Fraudsters

Common analysis – CPP finding

- **Common Point of Purchase (CPP)**
  - Where hackers manage to steal a group of cards for follow up fraud, usually via merchant compromise
  - This can happen in both CP (Card present) and CNP (Card not present) space.

Common analysis – CPP finding

- Example
  - Skimming is one example we face often in this space.



Common analysis – CPP finding

CNP (Merchant compromise)

Optus: How a massive data breach has exposed Australia

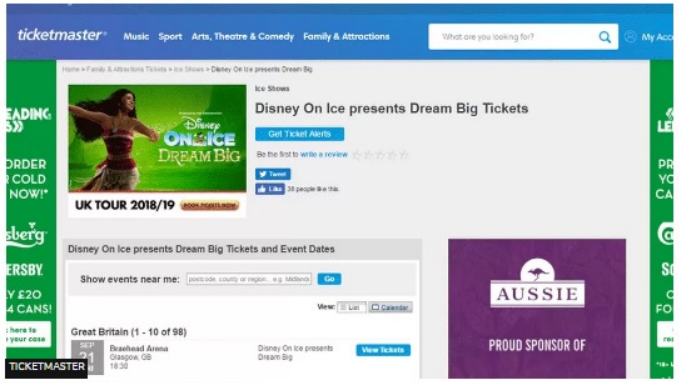
29 September 2022

Optus is the country's second-largest telecommunications company

By Tiffanie Turnbull
BBC News, Sydney

Ticketmaster admits personal data stolen in hack attack

27 June 2018



Ticketmaster sold 292 million tickets in 2017

Ticketmaster has admitted that it has suffered a security breach, which the BBC understands has affected up to 40,000 UK customers.

Addressing Fraud in Transactions

Problem Statement

Bank A faces significant challenges in detecting and responding to fraudulent transactions. The current fraud detection system struggles to keep up with evolving fraud patterns, leading to financial losses and erosion of customer trust.

Current Scenario

- Increase in online and mobile banking has led to a rise in sophisticated fraud schemes.
- Existing detection systems are sometimes unable to keep up with new fraud patterns.
- Impact:
  - Financial Losses: Significant monetary losses due to undetected fraud.
  - Customer Trust: Erosion of customer confidence in the bank's security measures.

Addressing Fraud in Transactions

Executive Summary

The project aims to enhance Bank A's fraud detection capabilities and improve the response process for suspected fraudulent transactions. This involves implementing advanced analytics to identify potential fraud and provide recommendations to Bank A about a customer response protocol to minimize financial losses and maintain customer trust.

Tips!

- What patterns you've observed from data?
- Exploratory analysis!
- Which matrix/matrices to use?
- What's the impact to customer?
- *Model explainability?