Imperial College London

Plastic Card Fraud Detection using Peer Group analysis

David Weston, Niall Adams, David Hand, Christopher Whitrow, Piotr Juszczak

29 August, 2007

EPSRC Think Crime Initiative

Imperial College London

- EPSRC Think Crime Initiative
- Crime Prevention & Detection
- Funding 12 projects
- Also feasibilty studies and more

Think Crime Project

- Develop Fraud Detection Tools
- Real Data

ThinkCrime Team

Imperial College London

- Members of the team are
  - David Hand
  - Niall Adams
  - Christopher Whitrow
  - Piotr Juszczak
  - David Weston
  - Gordon Blunt
- Collaborating banks
  - Abbey National, Alliance and Leicester, Capital One, Lloyds TSB

Overview

Imperial College London

- Peer Group Analysis
  - Introduction
  - Applied to Time-Aligned Multivariate Continuous Data
  - Applied to Credit Card Transaction Data
- Performance Evaluation
- Experiments & Results
- Conclusions & Current Work

Peer Group Analysis - Introduction

Approaches to Fraud Detection

Imperial College London

- Broadly 2 approaches to statistical fraud detection
- Supervised or Anomaly Detection

Approaches to Fraud Detection

Imperial College London

- Broadly 2 approaches to statistical fraud detection
- Supervised or Anomaly Detection
  - Supervised
    - Historical Instances of Fraud
    - Less likely to falsely flag a transaction as fraudulent
    - Approach Chris is taking

Anomaly Detection

Imperial College London

- Does not use historical Instances of Fraud
- Build a profile of ‘usual’ behaviour
- Significant deviations considered frauds
- More likely to falsely flag a transaction as fraudulent
- Potential to adapt to changing fraud patterns
- Approach Piotr is taking

Peer Group Analysis

Imperial College London

- Similar to anomaly detection methods
- Do not need to build a model of usual behaviour for account holder
- Determine a peer group
- Find other accounts that you expect will behave similarly to the account holder
- Find accounts that have behaved similarly in the past
- Monitor account holder's behaviour with respect to peer group
- Anomalous behaviour, should account holder deviate strongly from peer group

Anomaly Detection to Peer Groups I

Imperial College London

- The weekly amount spent on a credit card for a particular account
- Week 1 to Week n

$$y_1, \ldots, y_{n-1}, y_n$$

- Target Account
- Wish to determine if the amount spent in week n is anomalous

Anomaly Detection based on account profile

Anomaly Detection to Peer Groups II

Imperial College London

Population Normalised Anomaly Detection

$x_{m,1}$	$x_{m,2}$	$\cdots$	$x_{m,n-1}$	$x_{m,n}$
$\vdots$				
$x_{2,1}$	$x_{2,2}$	$\cdots$	$x_{2,n-1}$	$x_{2,n}$
$x_{1,1}$	$x_{1,2}$	$\cdots$	$x_{1,n-1}$	$x_{1,n}$
y_1	y_2	$\cdots$	y_{n-1}	y_n

Anomaly Detection to Peer Groups III

Imperial College London

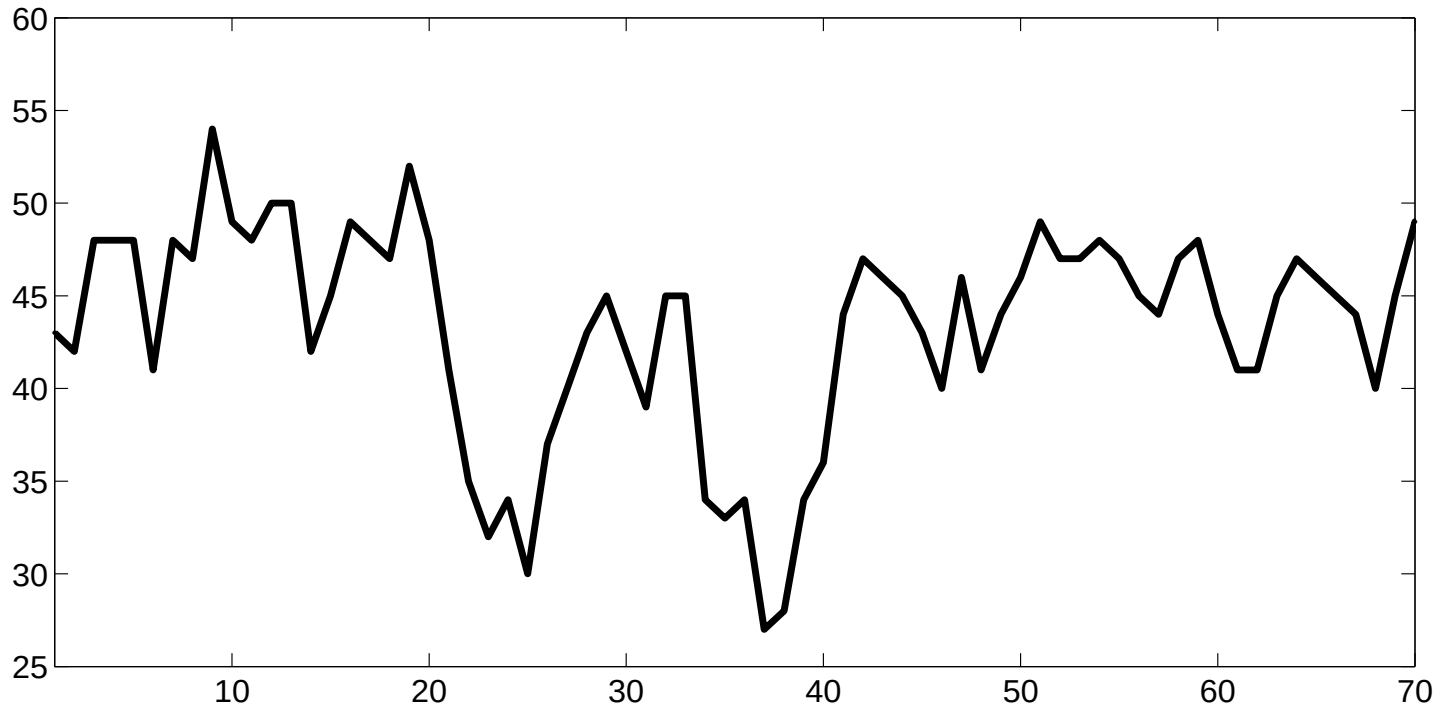
Sort accounts in order of decreasing similarity, $\pi(i)$

$x_{\pi(m),1}$	$x_{\pi(m),2}$	$\cdots$	$x_{\pi(m),n-1}$	$x_{\pi(m),n}$
$\vdots$				
$x_{\pi(k),1}$	$x_{\pi(k),2}$	$\cdots$	$x_{\pi(k),n-1}$	$x_{\pi(k),n}$
$\vdots$				$\vdots$
$x_{\pi(2),1}$	$x_{\pi(2),2}$	$\cdots$	$x_{\pi(2),n-1}$	$x_{\pi(2),n}$
$x_{\pi(1),1}$	$x_{\pi(1),2}$	$\cdots$	$x_{\pi(1),n-1}$	$x_{\pi(1),n}$
y_1	y_2	$\cdots$	y_{n-1}	y_n

- Peer Group size k

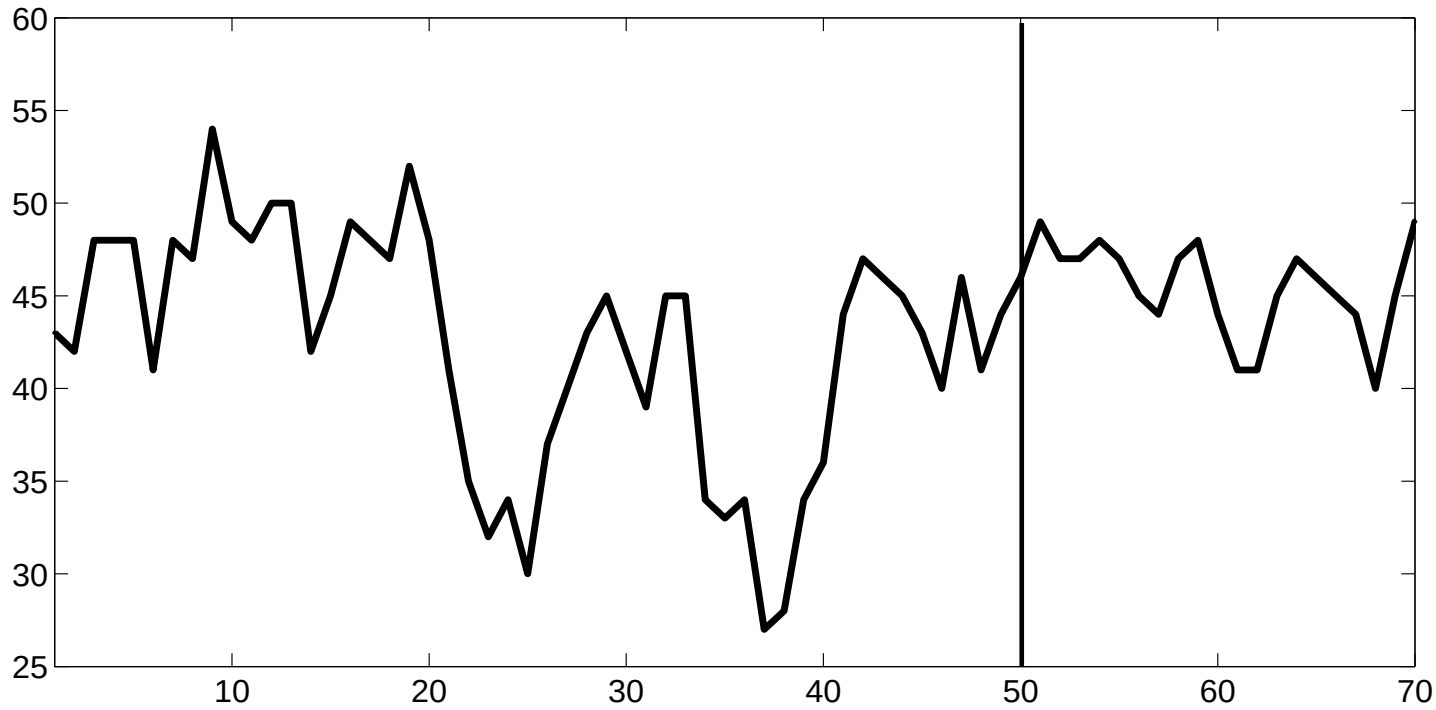
Peer Groups Example

Imperial College London



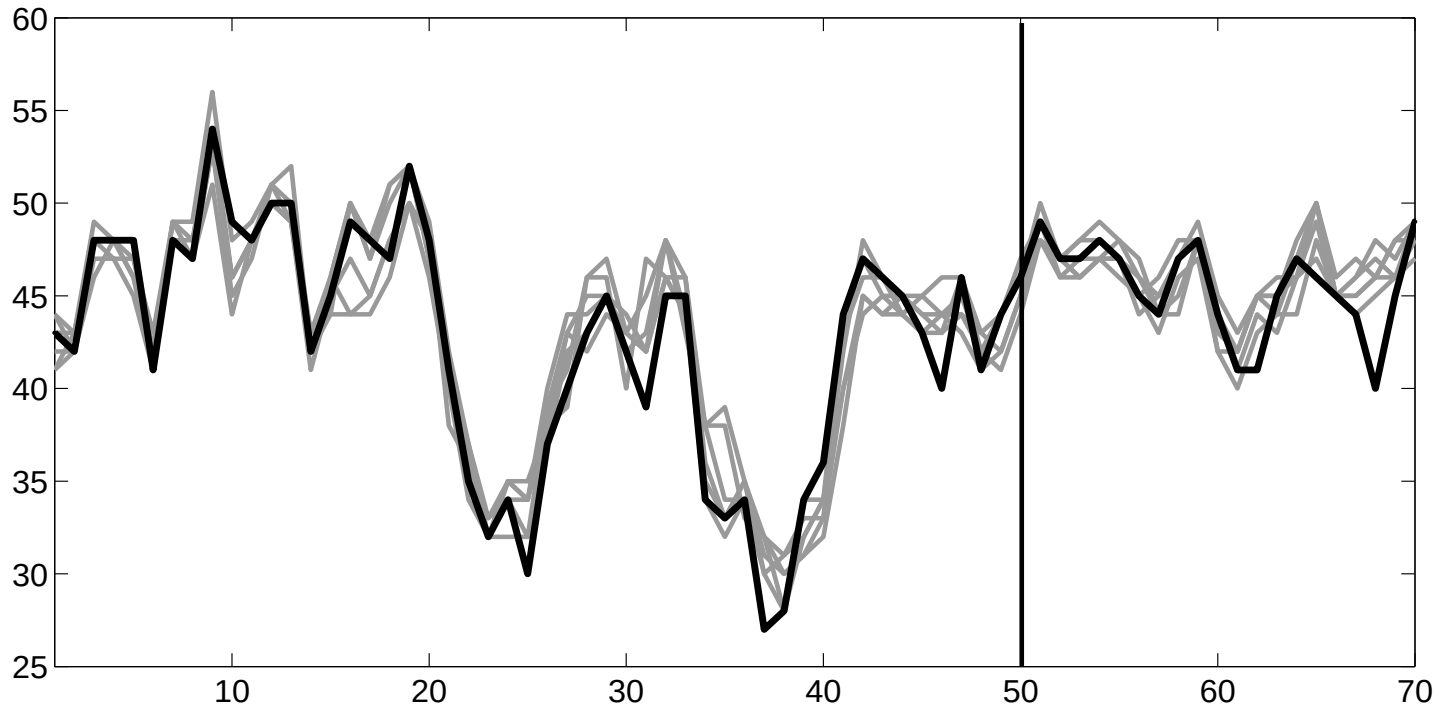
Peer Groups Example

Imperial College London



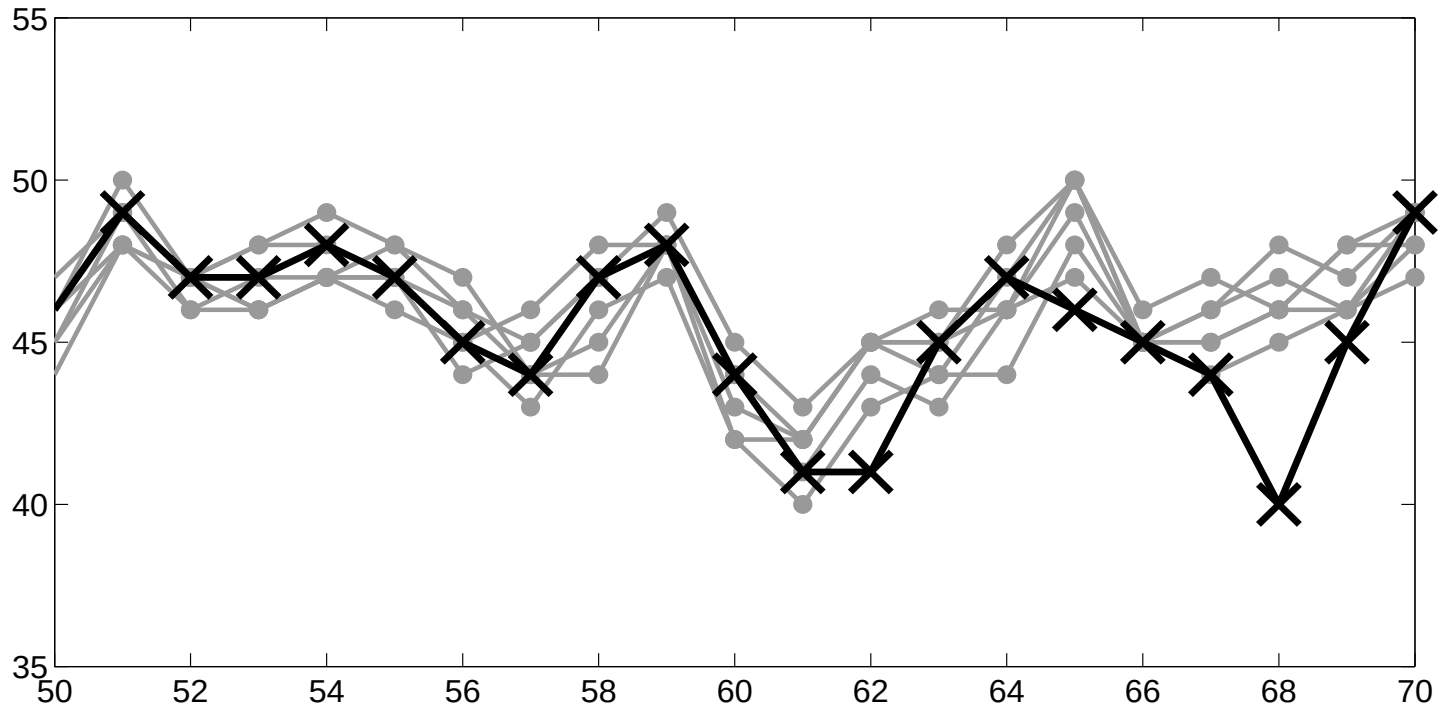
Peer Groups Example

Imperial College London



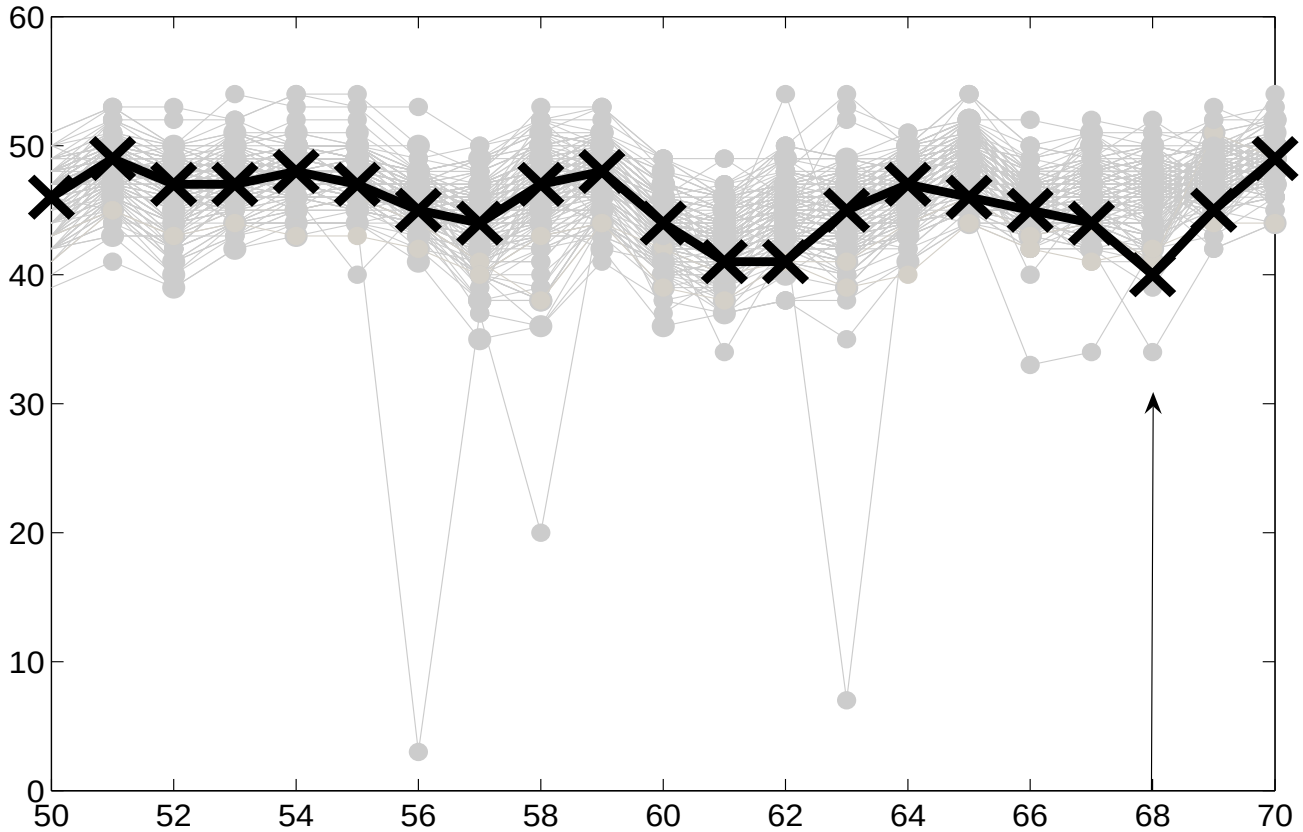
Peer Groups Example

Imperial College London



Peer Groups Example

Imperial College London



Peer Group Analysis

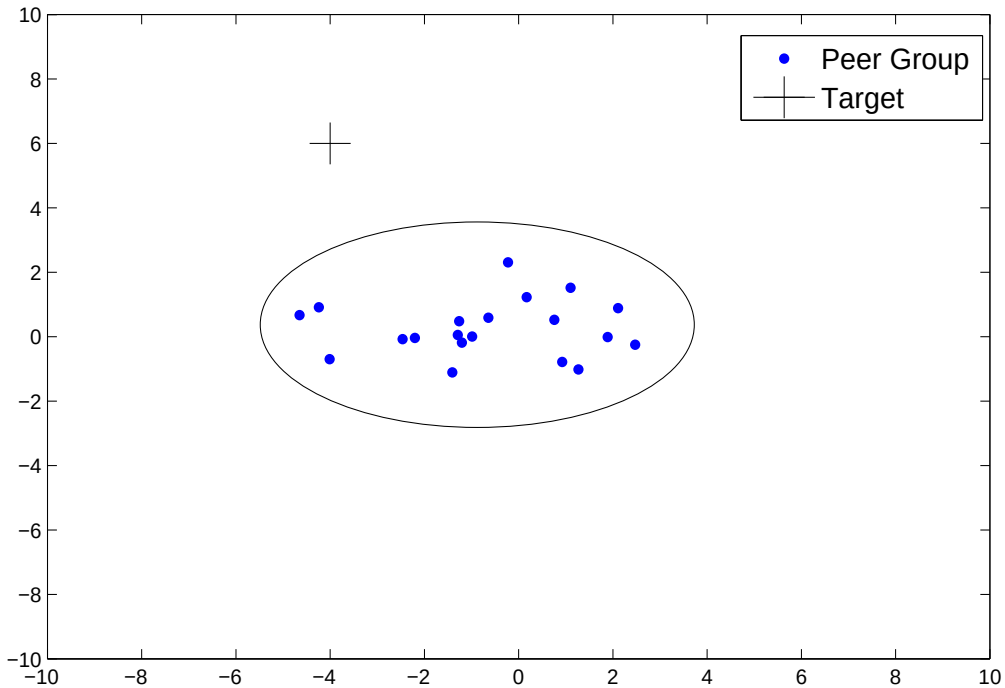
Detecting Anomalies

- Assuming we already have a peer group set of accounts for our target account.
- y_n is multivariate (column vector) and continuous
- Mahalanobis distance of the target from the mean of its peer group
- μ is mean of $x_{\pi(1),n}, \ldots, x_{\pi(k),n}$
- C is covariance matrix of $x_{\pi(1),n}, \ldots, x_{\pi(k),n}$
- Mahalanobis distance of a target from its peer group
  - $\sqrt{(y_n - \mu)^T C^{-1} (y_n - \mu)}$

Detecting Anomalies

Imperial College London

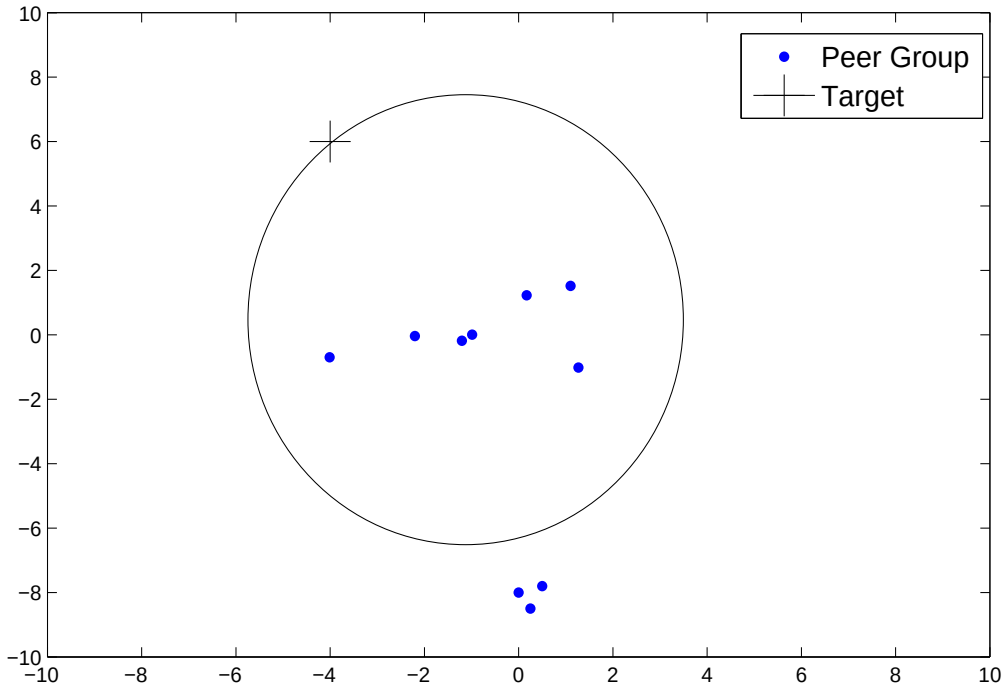
- If the distance is above an externally selected threshold, then we flag the target as fraudulent.



Robustifying Peer Groups

Imperial College London

- Peer Group contaminated by fraudulent transactions
- Outlier Masking
- Outlier Swamping



Robustifying Peer Groups

Imperial College London

- Robustify the covariance matrix for the Mahalanobis Distance evaluation
- Use Heuristic

Robustifying Peer Groups

Imperial College London

- Robustify the covariance matrix for the Mahalanobis Distance evaluation
- Use Heuristic
- An account that has deviated strongly from its peer group at time t should not contribute to any peer group at time t

Robustifying Peer Groups

Imperial College London

- Robustify the covariance matrix for the Mahalanobis Distance evaluation
- Use Heuristic
- An account that has deviated strongly from its peer group at time t should not contribute to any peer group at time t
- For each peer group select 75% closest to their own peer groups

Peer Group Quality

It is not necessarily the case that peer group analysis can be successfully deployed on all accounts.

$$q_t = \frac{1}{k} \sum_{i=1}^{k} (y_t - x_{\pi(i),t})^T (y_t - x_{\pi(i),t}) \quad (1)$$

where T is the transpose. This is a simple measure of how close the members of the peer group are to the target.

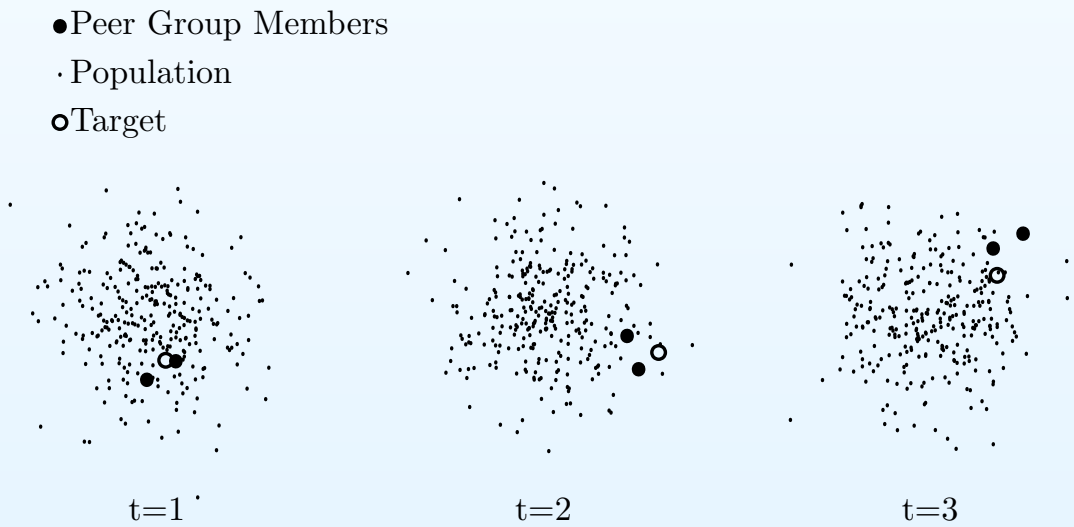
- A good quality peer group is one that closely follows the target over time.

$$Q_{s,e} = \frac{1}{t_e - t_s} \sum_{t=t_s}^{t_e} q_t. \quad (2)$$

Whitening the Population

Imperial College London

- Whitening the population to make the scatter of a peer group (of size 2) commensurate across time
- The smaller the value of $Q_{s,e}$ the better the peer group tracks the target over time.



Building Peer Groups

Imperial College London

- Possible to know apriori the peer group membership
- Employee fraud detection, people with the same job description can be naturally grouped together.
- IBM FAMS. Health care fraud. Geography, speciality
- Infer peer group membership from the time series itself
- Measuring similarity of time series

Applying Peer Group Analysis

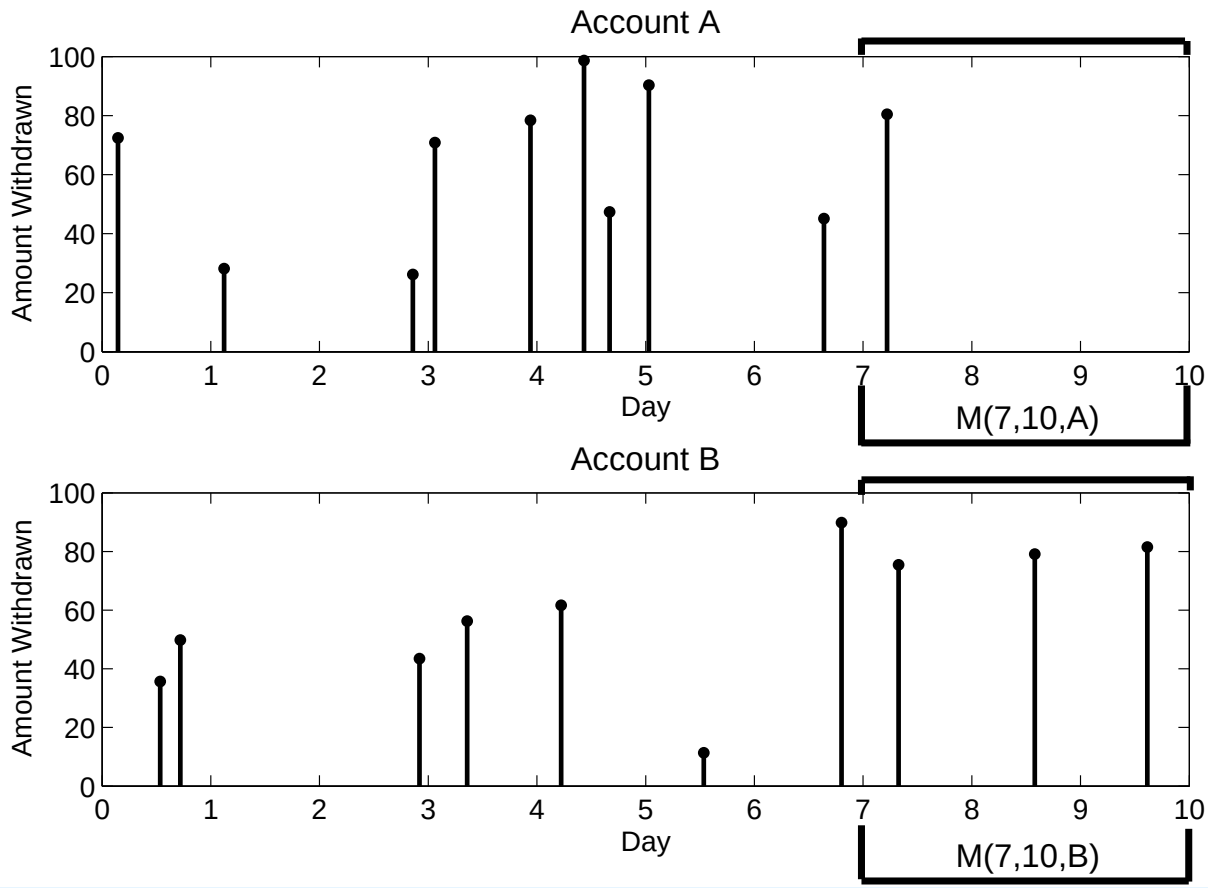
Time Alignment & Feature Extraction

Imperial College London

- Accounts' transactions are asynchronous data streams
- Synchronise account time series by extracting features from the data streams at regular time intervals
- $M(s, e, A)$ summarise transactions of account A occurring from day s to day e inclusive
  - Mean amount spent
  - Number of transactions
  - Entropy of Merchant Category Groups
    - 16 Groups +1 for ATMs
- Returns 1 point in 3 dimensional space

Time Alignment & Feature Extraction

Imperial College London



Outlier Detection from Peer Groups

Imperial College London

- Once a day at midnight
- Summary statistic for day t, behaviour of the past d days $M(t-d+1, t, A)$
- Smaller d, the more sensitive to new transactions
- Mahalanobis distance in 3 dimensional space

Active and Inactive Accounts

Imperial College London

- Account inactive on day t if it has not performed any transactions on that day
- Do not test for outlierness for inactive accounts
- Unusually long periods of inactivity will not be considered fraudulent

Active and Inactive Accounts

Imperial College London

- Account inactive on day t if it has not performed any transactions on that day
- Do not test for outlierness for inactive accounts
- Unusually long periods of inactivity will not be considered fraudulent
- Account not active over entire summary statistic window
- Active peer group members. Closest k accounts that are active on at least one day of the summary statistic window

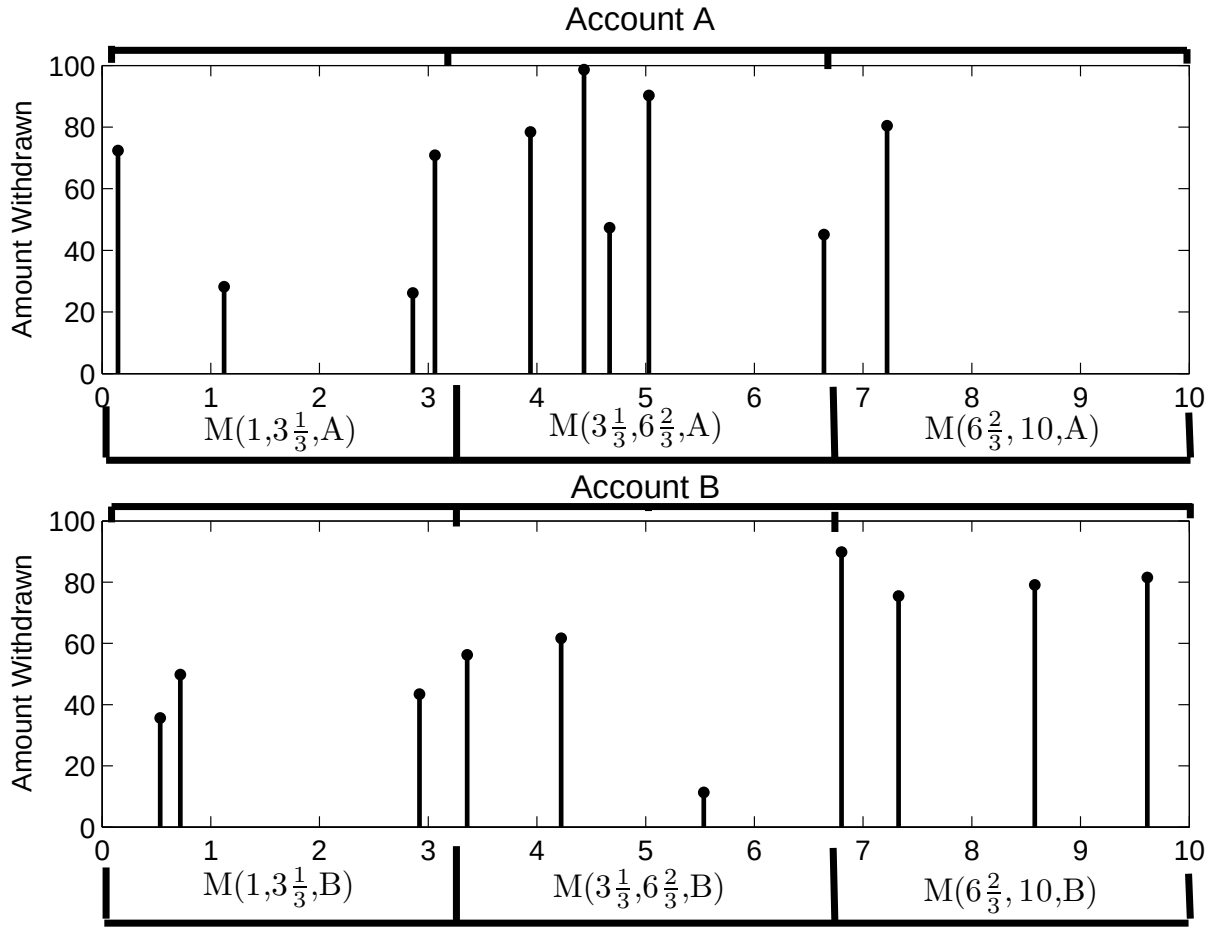
Building Peer Groups

Imperial College London

- Subdivide training data into n non-overlapping windows
  - $M(1, \frac{L}{n}, A), \ldots, M((n-1)\frac{L}{n} + 1, L, A)$
- Point in $3n$ dimensional space
- Complication, potential for bias
- Standardise each window by whitening

Building Peer Groups

Imperial College London



Building Peer Groups

Imperial College London

- Find k nearest neighbours
- Large number of accounts
- Accounts that have high volume of transactions unlikely to be tracked by accounts with low volume
- First sort by number of transactions in training data

Performance Evaluation

Performance Criteria

Imperial College London

- Reduce total amount lost to fraud
- Reduce number of fraudulent transactions
- Reduce the time between fraud starting and fraud detection
- Reduce the number of account holders affected by flagging legitimate transactions as fraud
- Number of possible performance metrics

Performance Metric

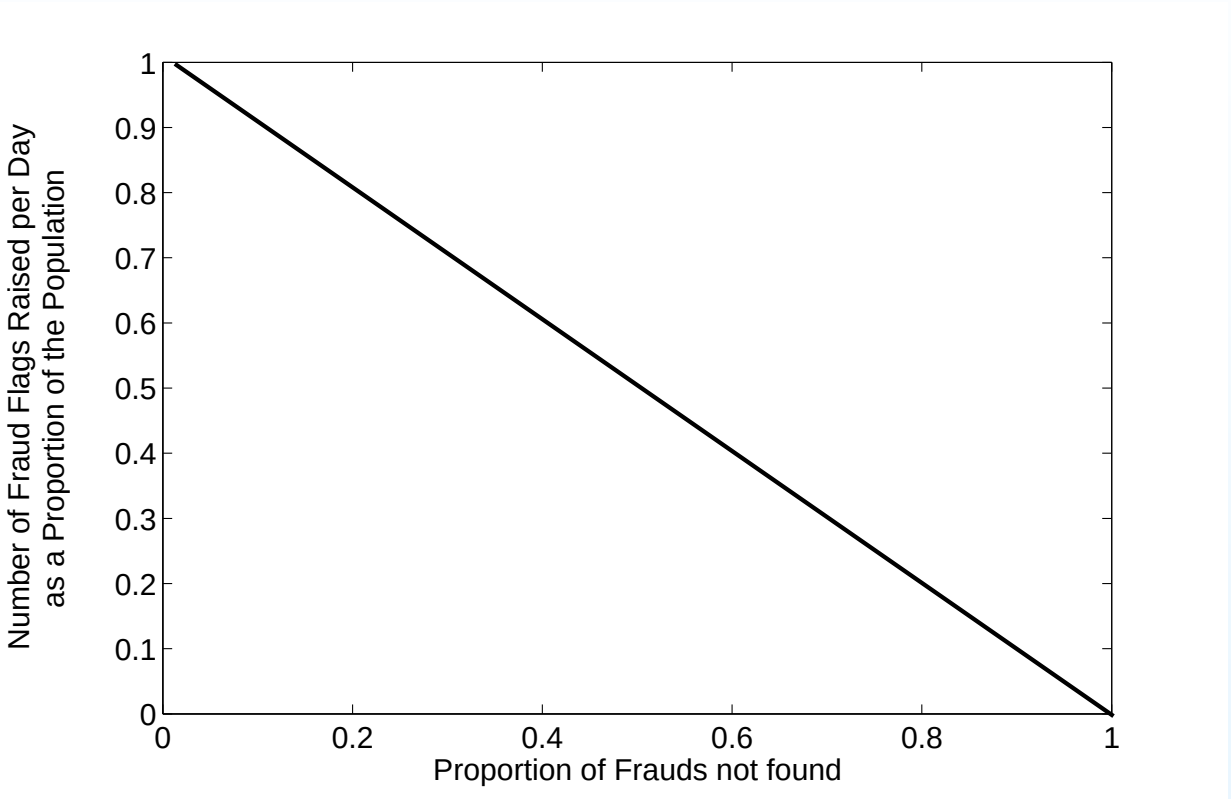
- If an account has been flagged as containing fraudulent transactions. The card issuer would need to investigate this account.
- minimise the amount of fraud given the number of investigations the card company can make

Performance Curve

- x-axis number of fraudulent accounts missed as a proportion of the number of fraudulent accounts
- y-axis number of fraud flags raised as a proportion of the number of accounts
- Different to ROC curve. The smaller the area under the curve the better the performance.
- Random classification is represented by a diagonal line from the top left to the bottom right.

Performance Curve

Imperial College London

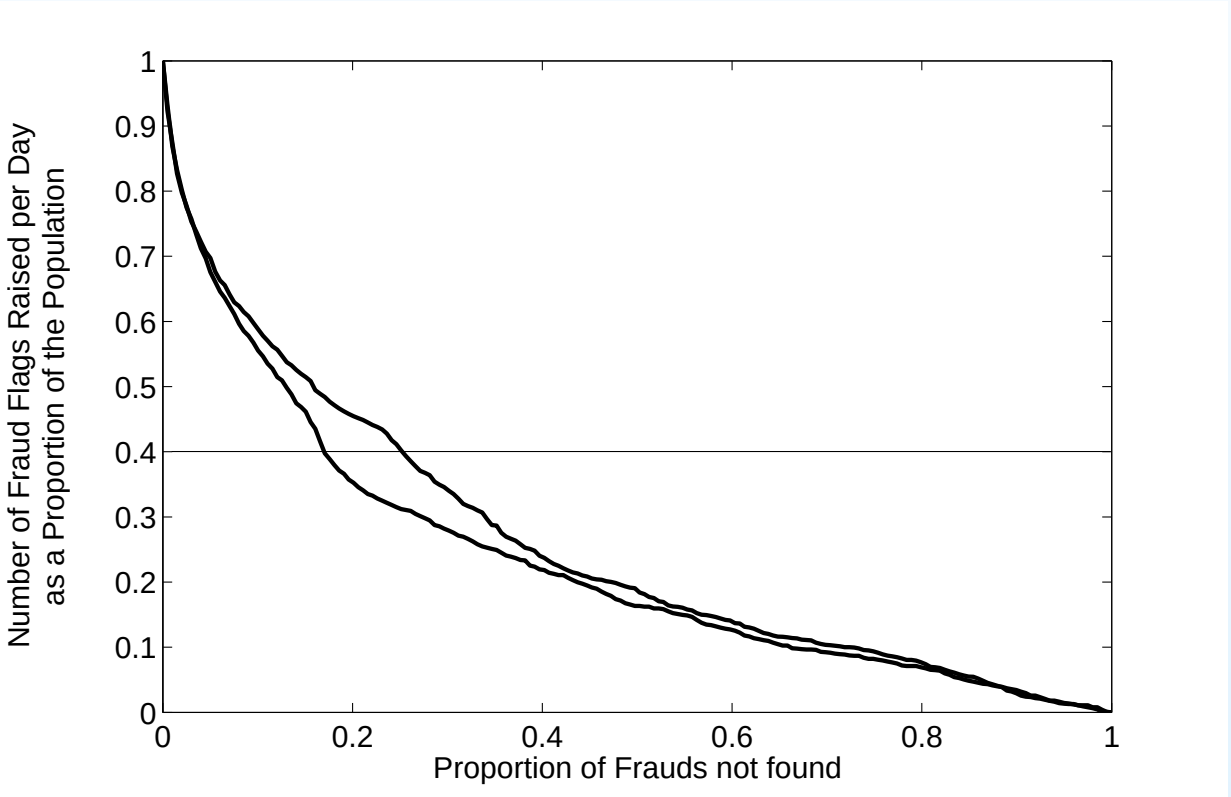


- The lower the curve the better the performance.
- Twice Area under Curve [0,1], smaller the area the better the performance

Average Performance Curve

Imperial College London

- Produce one curve for each day
- Take the average of the curves.
- For a given proportion of fraud flags raised



Experiments & Results

Experiments

Imperial College London

Data

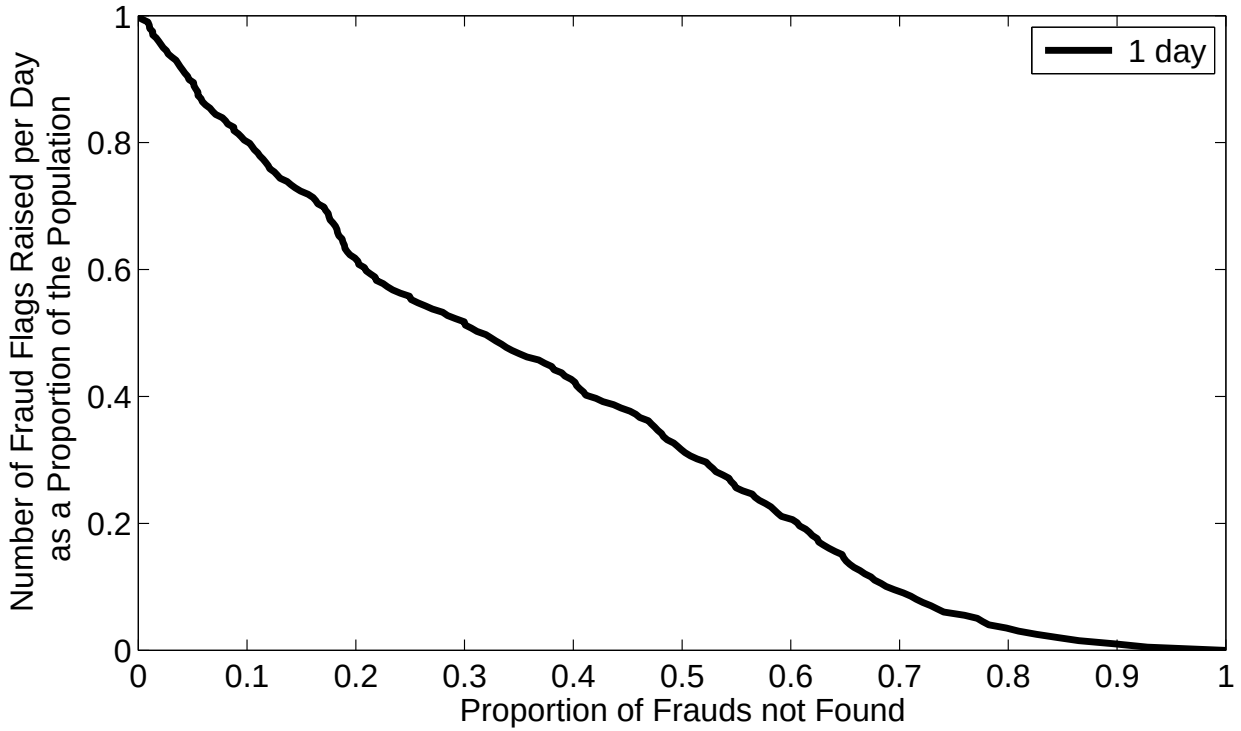
- 4 months of data
- Accounts with > 80 transactions and fraud free for first 3 months.
- About 4000 accounts 6% defrauded in final month
- Performed Peer Group Analysis once a day for the remaining month

Parameters

- Peer Group building 8 segments
- Summary Statistic window size 7 days
- Active Peer Group Size 100
- Robustifying Peer Groups not used

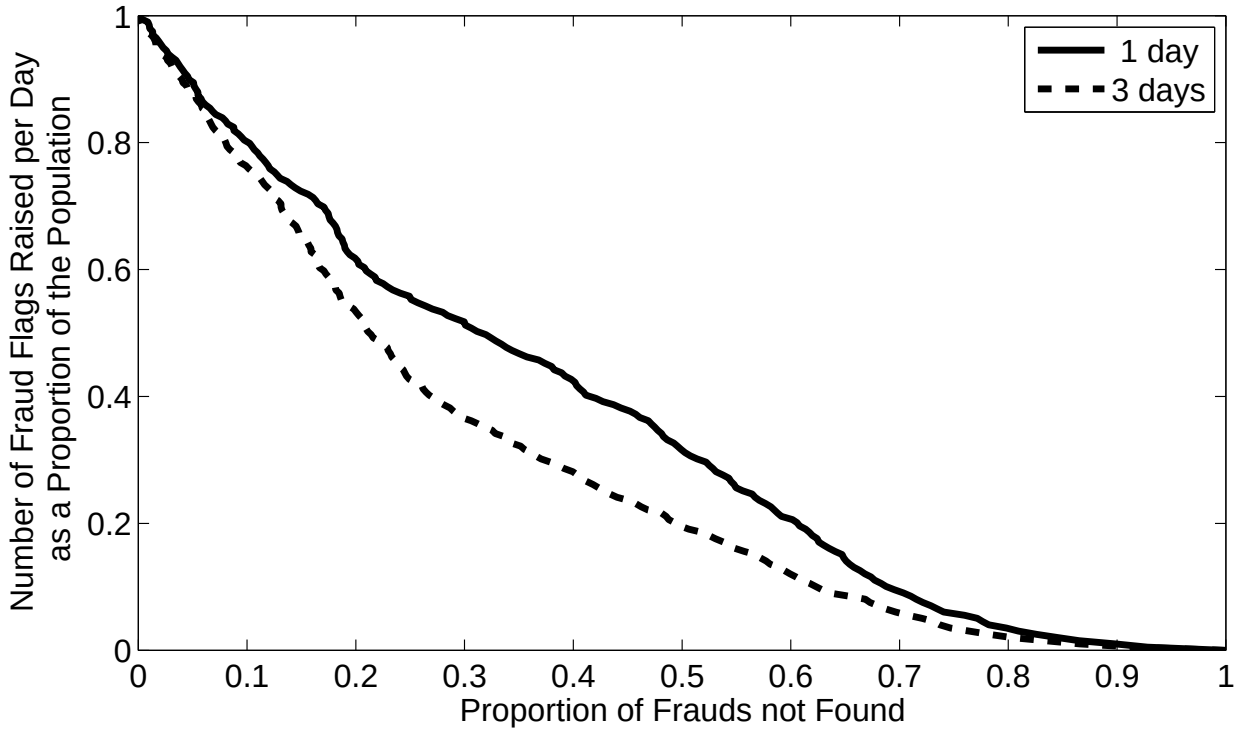
Varying Length of Summary Statistic Window

Imperial College London



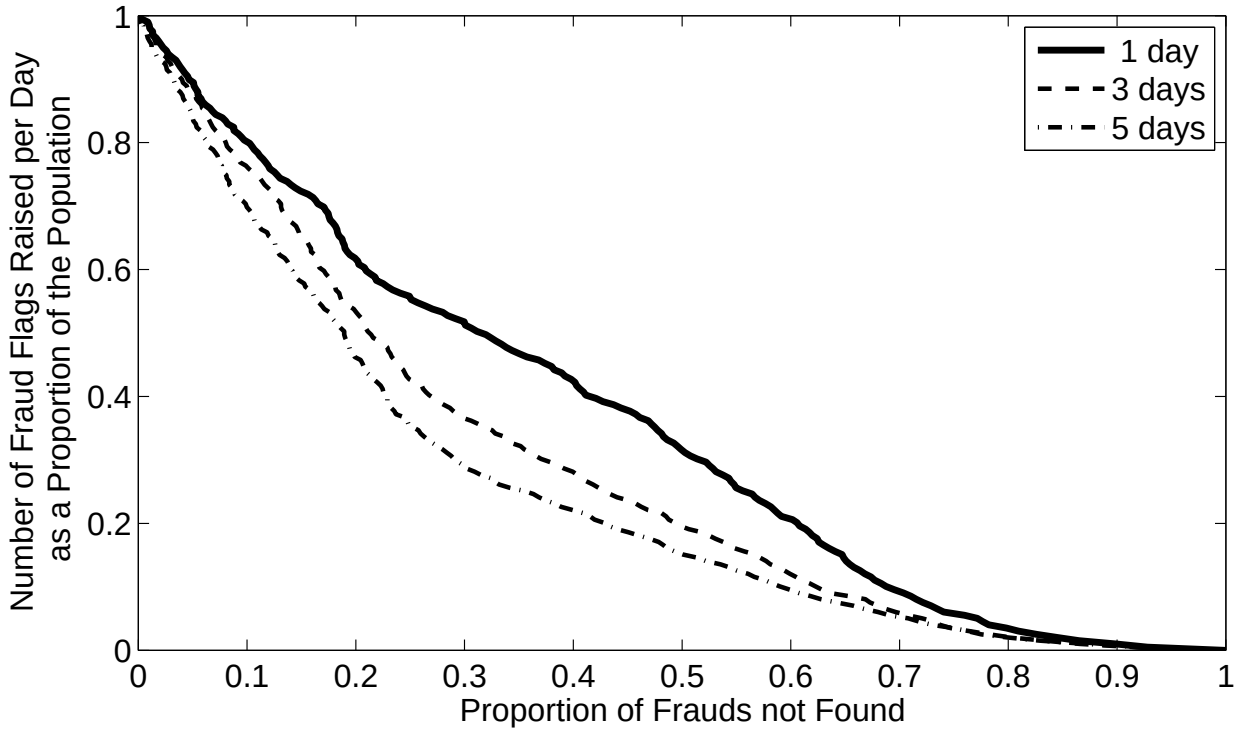
Varying Length of Summary Statistic Window

Imperial College London



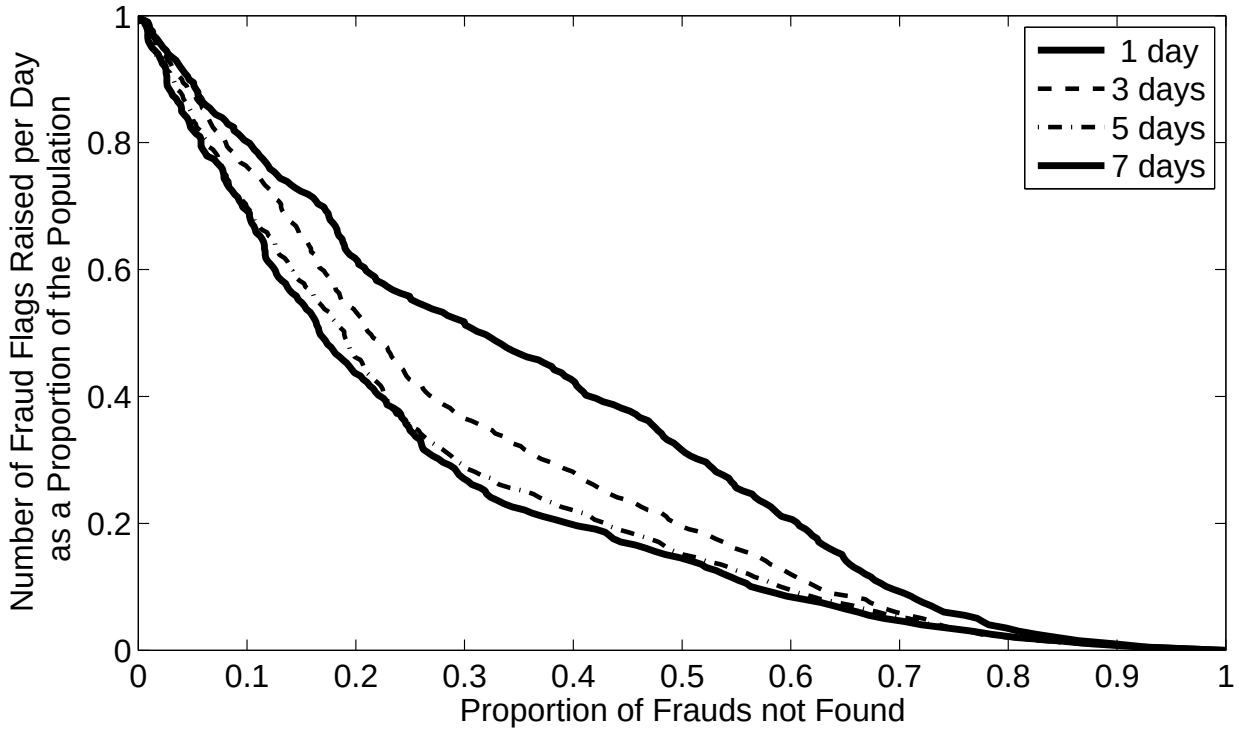
Varying Length of Summary Statistic Window

Imperial College London



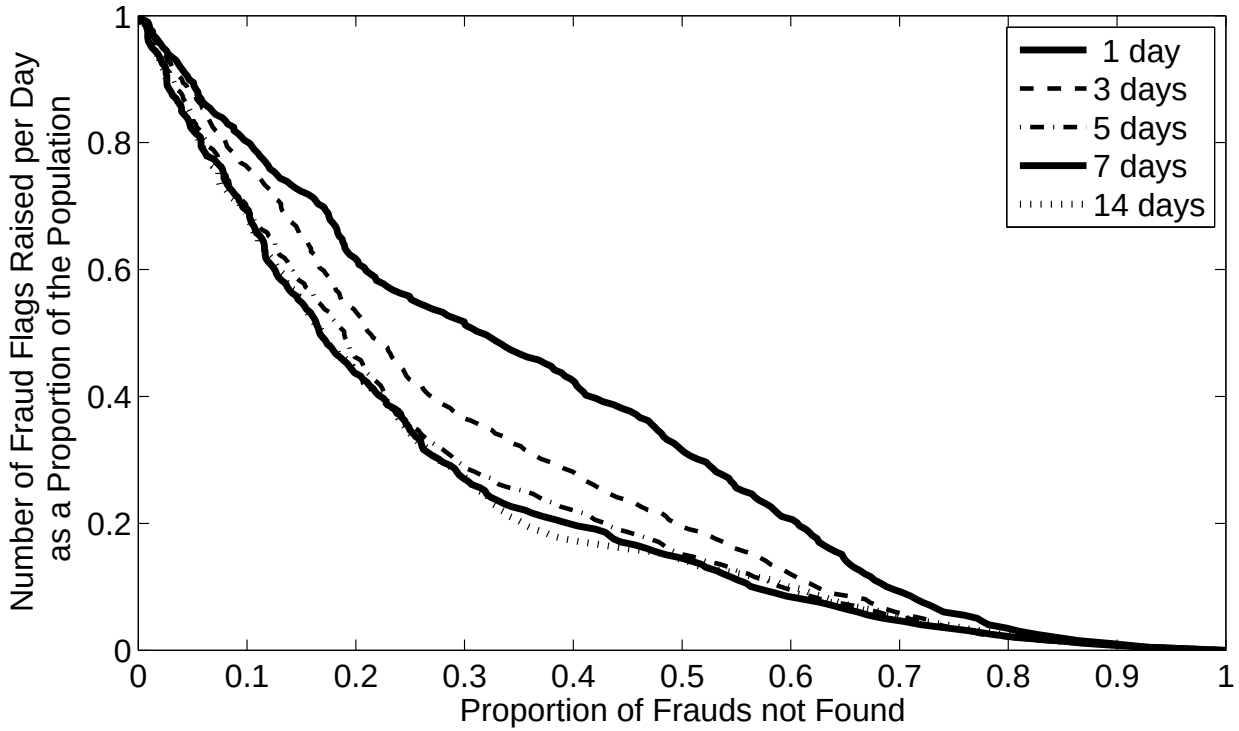
Varying Length of Summary Statistic Window

Imperial College London



Varying Length of Summary Statistic Window

Imperial College London



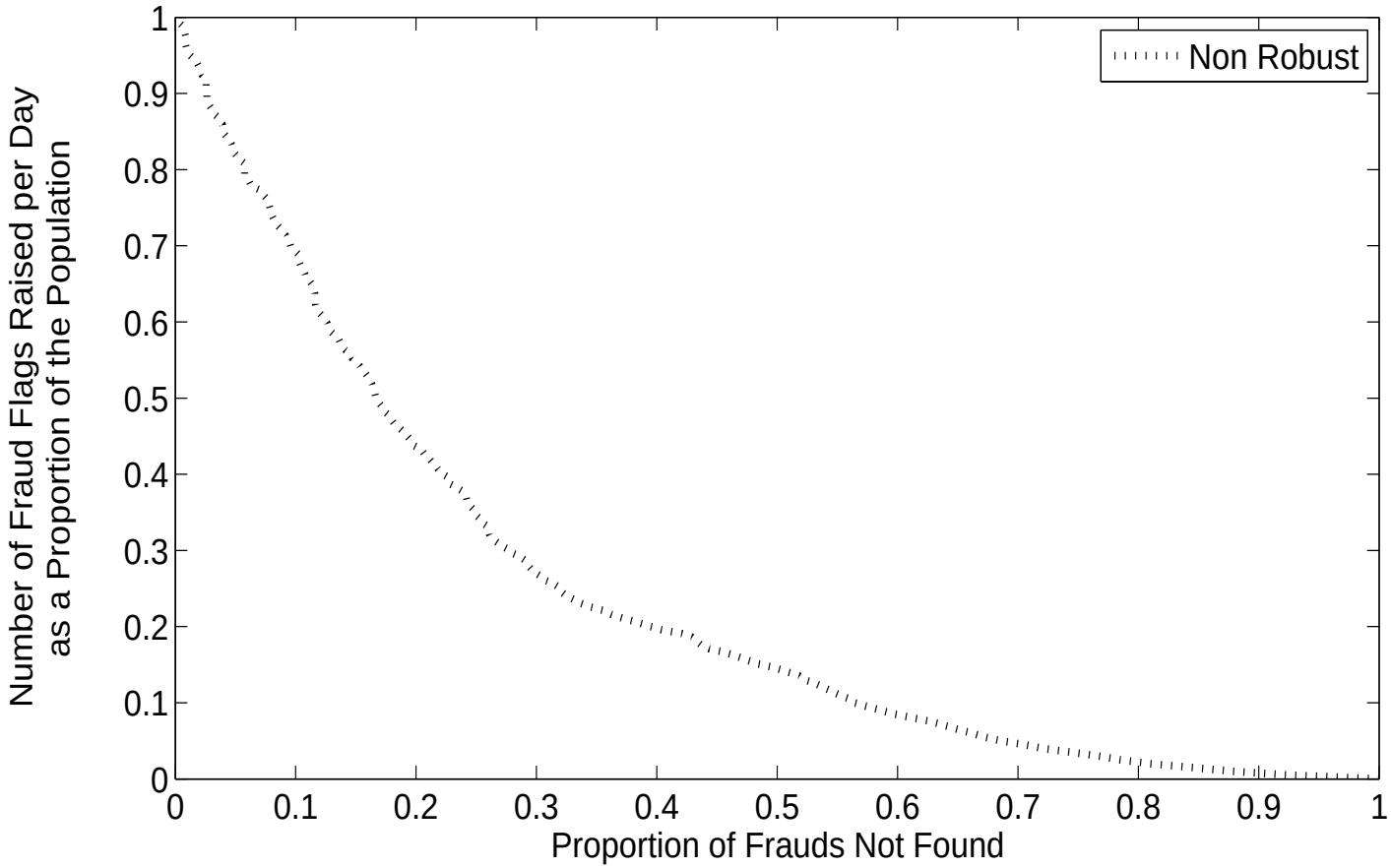
Global Outlier Detector

Imperial College London

- Is peer group analysis doing nothing more than finding outliers to the population?
- Special case, use largest possible peer group
- All accounts apart from target account
- Subtract Performance Curve for Peer Group from Global.
- Values less than zero imply Peer Group method is performing better.

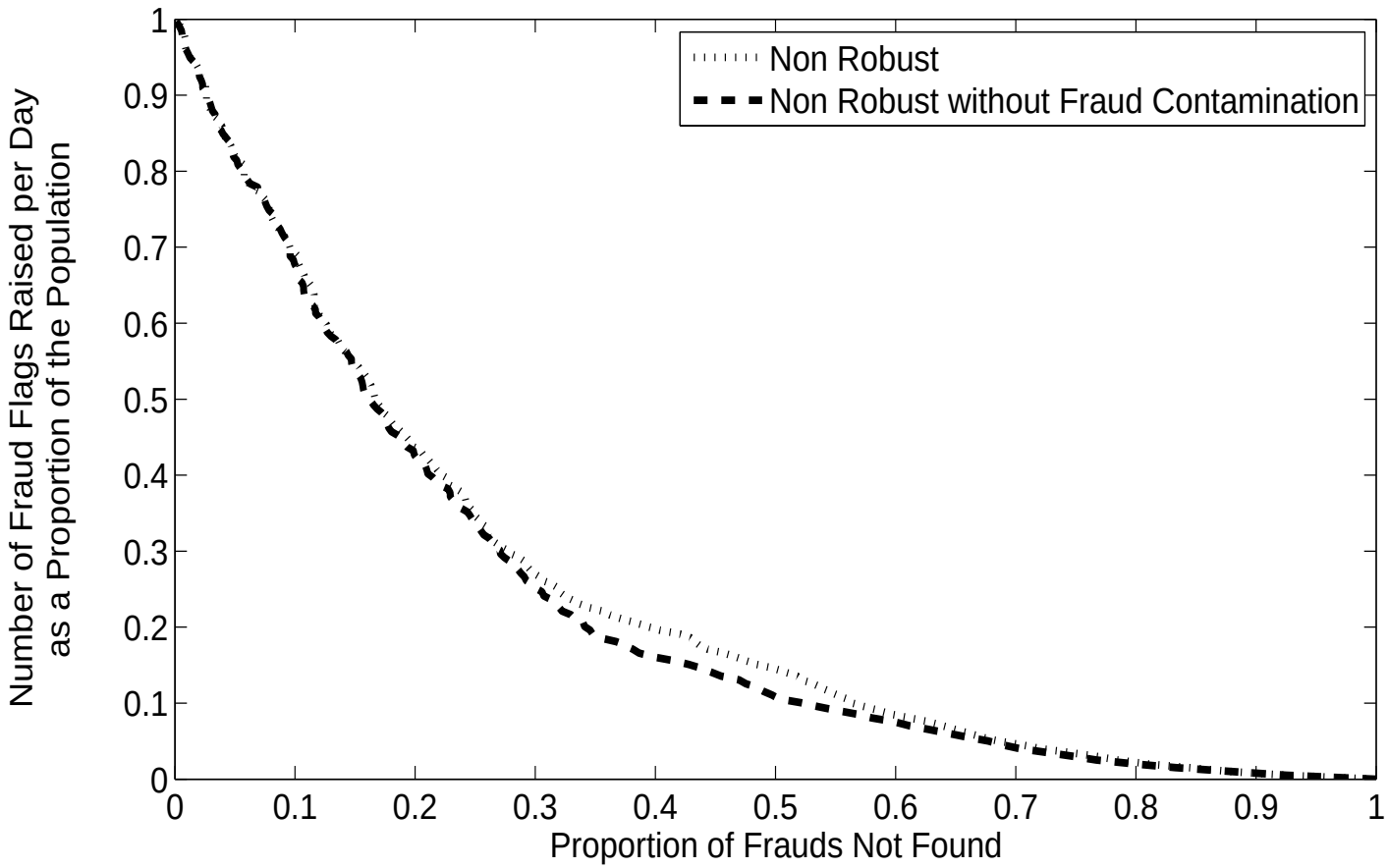
Peer Groups Performance

Imperial College London



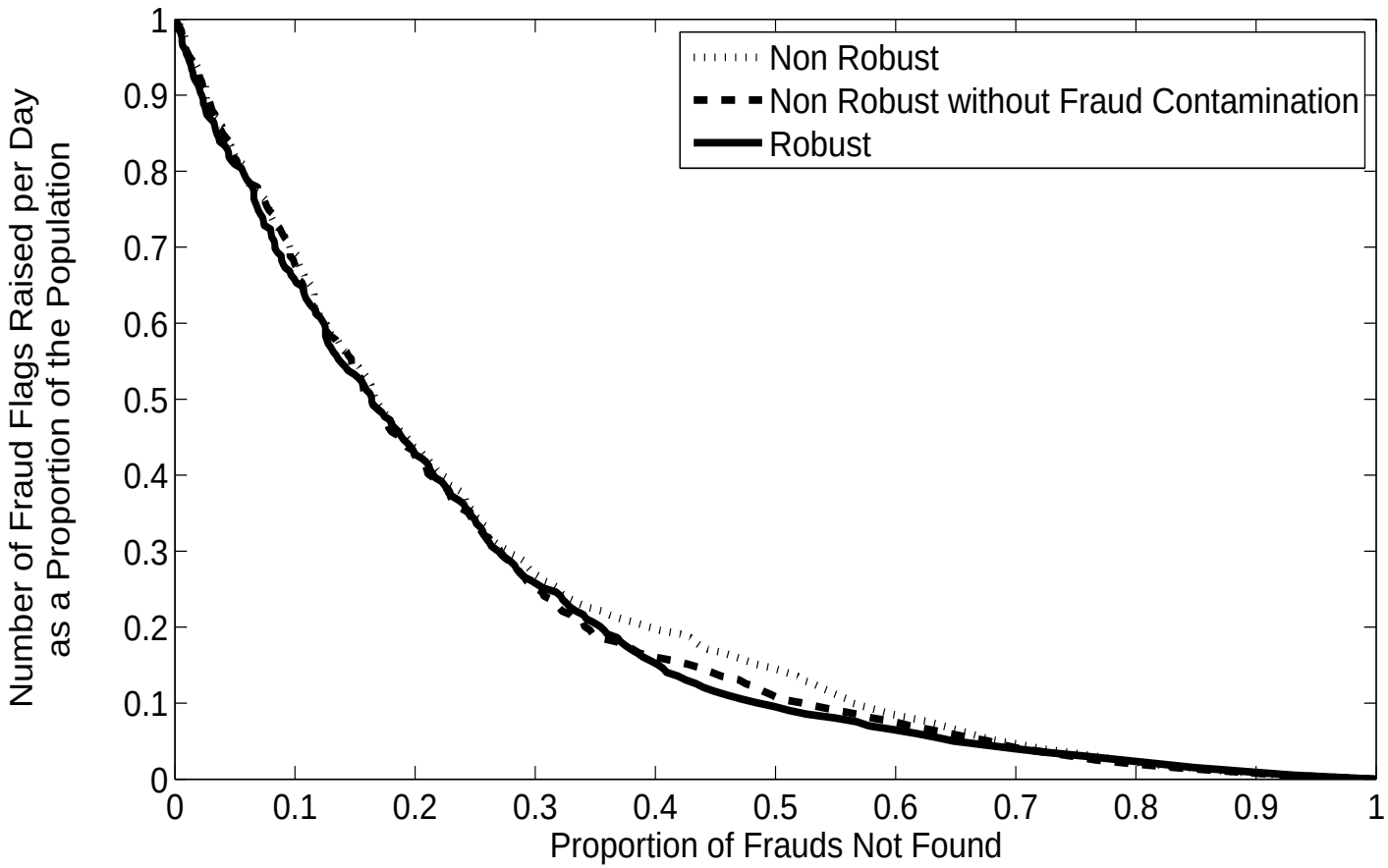
Peer Groups Performance

Imperial College London



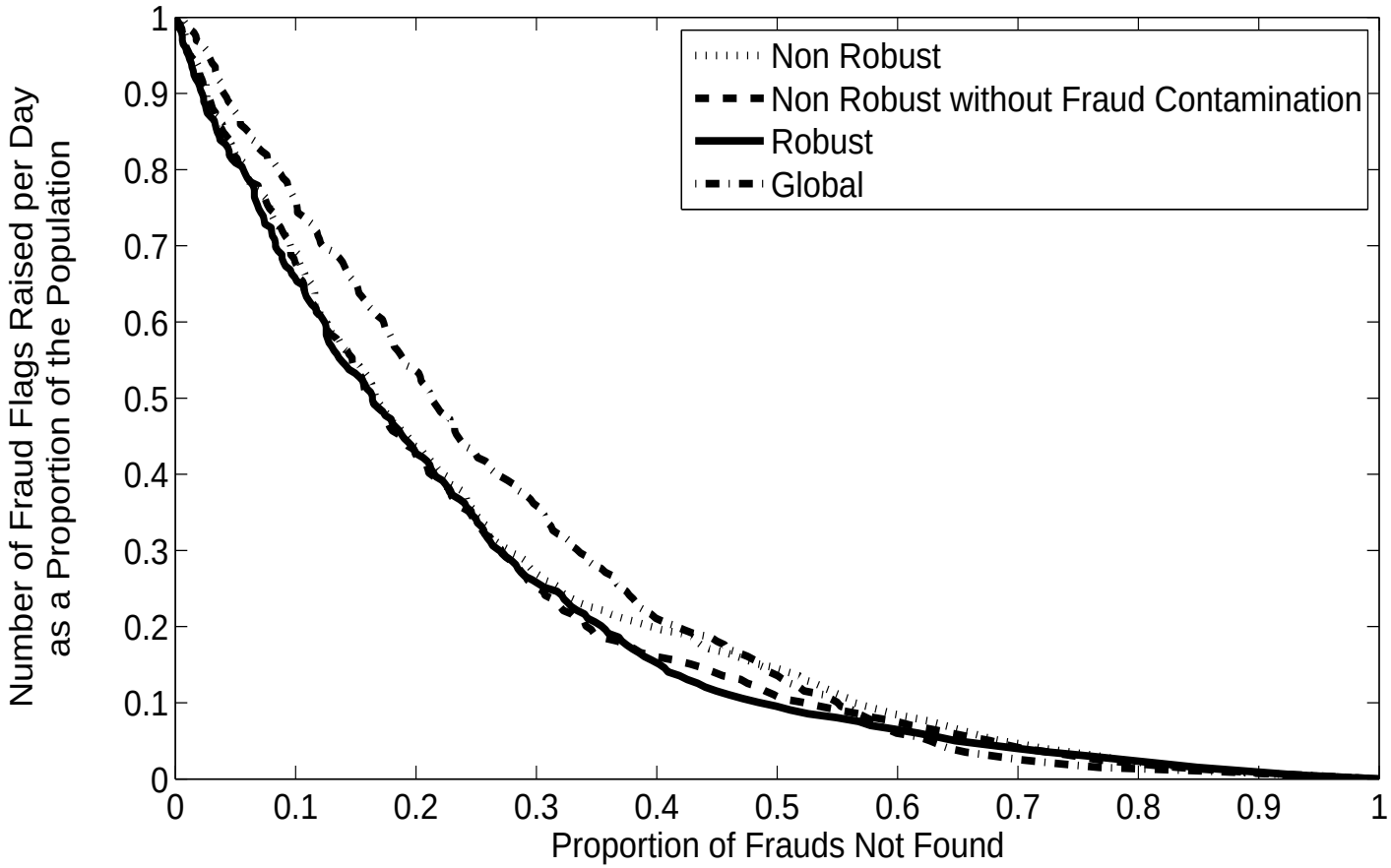
Peer Groups Performance

Imperial College London



Peer Groups Performance

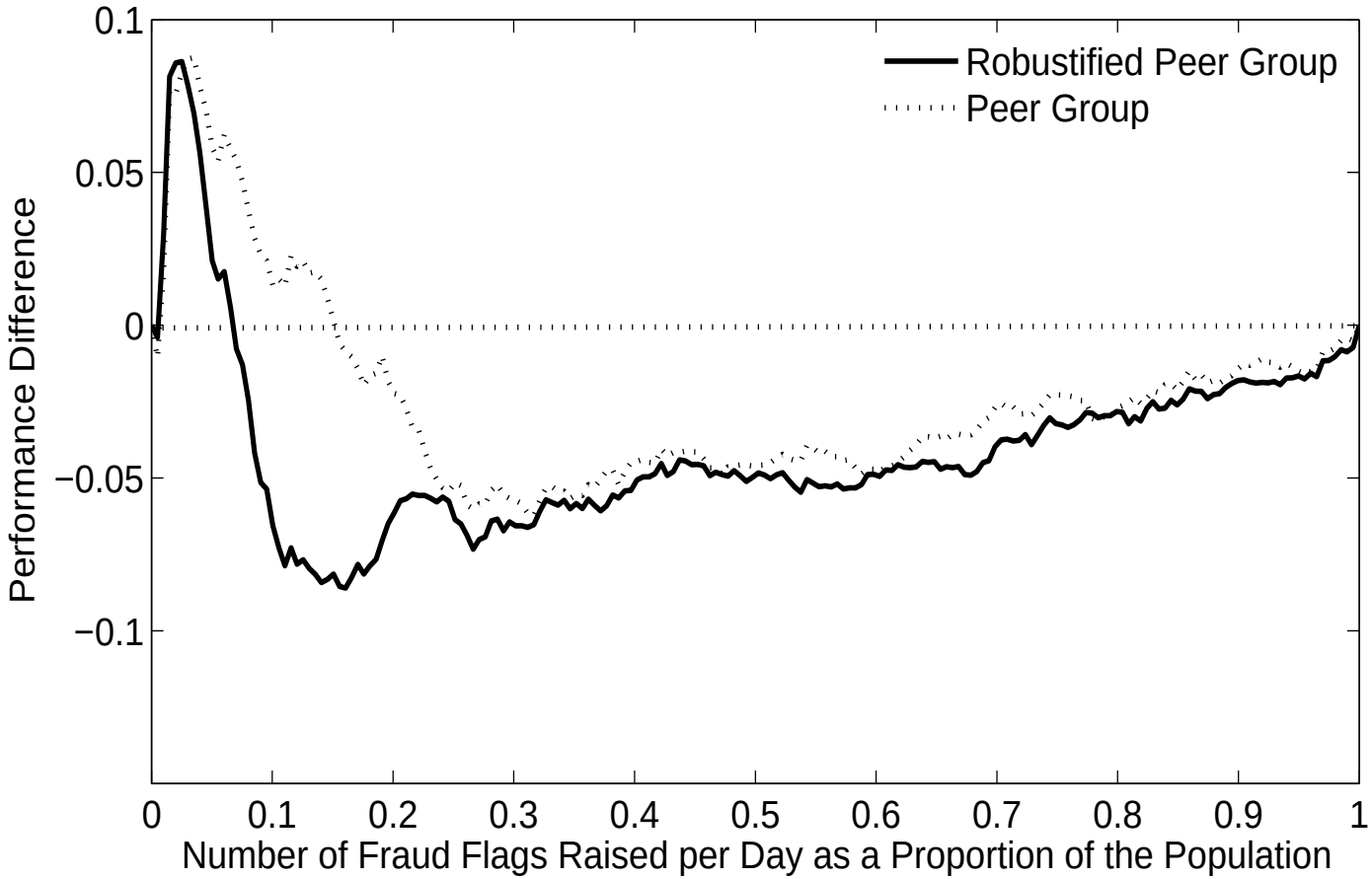
Imperial College London



Peer Groups Versus Global Outlier Detector

Imperial College London

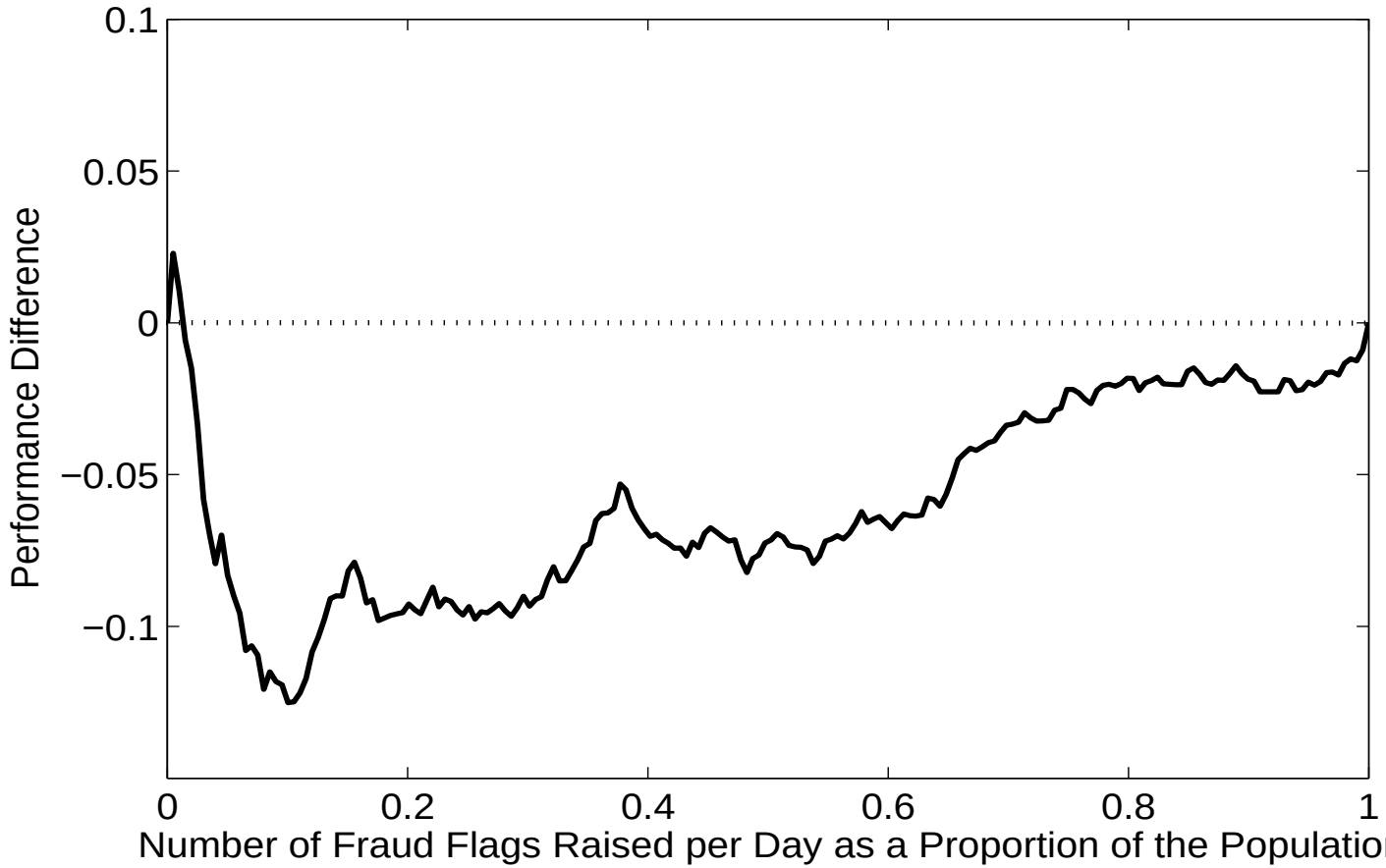
Performance of the peer group analysis compared with global population outlier detector.



Peer Groups Versus Global Outlier Detector

Imperial College London

Performance of the robustified peer group analysis compared with global population outlier detector on screened data.



Conclusions & Current Work

Conclusions

Imperial College London

- We have demonstrated there exist credit card transaction accounts that evolve sufficiently closely to enable fraudulent behaviour to be detected.
- Finding frauds that are not global outliers to the population.

Current work

- Combining Methods

1 Day Symposium, 23rd November 2007

Imperial College London

Statistical and machine learning approaches to detecting fraud and predicting consumer behaviour

- Competing Risks in Retail Finance, *Crowder MJ*
- Event History Analysis for Debt Collection Portfolios, *Zhou F, Hand DJ, Heard NA*
- A dynamic scorecard for monitoring baseline performance with application to tracking a mortgage portfolio, *Whittaker J, Whitehead C, Somers M*
- Estimating the iceberg: how much fraud is there in the UK? *Blunt G, Hand DJ*
- Evaluating Fraud Detection Systems, *Hand DJ*
- Transaction Aggregation: A Winning Strategy vs. Fraud? *Whitrow C, Weston D, Juszczak P, Hand DJ, Adams N*
- Detecting Plastic Card Fraud using Peer Group Analysis, *Weston D, Whitrow C, Juszczak P, Hand DJ, Adams N*
- Behavioural finance as a multi-instance learning problem,*Juszczak P, Hand DJ*