Fraud in retail financial services
- prevention and detection

David J. Hand
Imperial College London

November 2008
Fraud is

*Criminal deception; the use of false representations to gain an unjust advantage*

Concise Oxford Dictionary

Older than humanity itself:
- even animals are known to try to deceive others
- camouflage
Six important issues in retail banking fraud

1) most transactions not fraud (needle in haystack)
2) fraud is a dynamic detection problem
3) the ‘economic imperative’
4) the Pareto principle
5) invisibility of fraud; visibility of detection
6) resources available for fraud detection are limited
   - in the UK around 3% of police resources go on fraud
   - this will not significantly increase
Many types of fraud

Motivation: money
Banking fraud
Telecoms fraud
Insurance fraud

Investment banking
Consumer banking

Money laundering
Credit card fraud
Mortgage fraud
Car finance fraud

Staff fraud
Identity theft

Card not present
Counterfeit
Lost
Mail non receipt

Internet fraud

Phishing
Advance fee fraud

Tax fraud
Auction fraud

Motivation: ideology, power, reputation
Terrorism
Science
So we have to be clever and out-think the fraudsters.

Use advanced technology and make their life difficult
Context:
Estimates of total cost of UK fraud range £7 bn to £70 bn
£630m of fraud brought to UK courts in first half 2008

Plastic Card Quarterly figures, end June 2008
1.8 bn plastic card purchases
£92.6 bn value of plastic card purchases
746 mn ATM withdrawals
£45.9 bn value of ATM withdrawals
1.4 bn automated payments
£21 tn value of automated payments

(APACS 18 August 2008)
About 1/1000 transactions are fraudulent

2006

- total card fraud loss £428 mn
- counterfeit £99.6 mn
- card-not-present £212.6 mn (and increasing)
How much does fraud cost?

Cost of fraud

= immediate direct loss due to fraud
  + cost of fraud prevention and detection
  + cost of lost business (when replacing card)
  + opportunity cost of fraud prevention/detection
  + deterrent effect on spread of e-commerce
Nature of plastic card fraud data

- many transactions - billions - algorithms must be efficient
- large number of variables
- different misclassification costs
- many ways of committing fraud
- unbalanced class sizes (c. 0.1% transactions fraudulent)
- delay in labelling
- mislabelled classes
- random transaction arrival times
- (reactive) population drift
Many variables:

Transaction ID
Transaction type
Date and time of transaction (to nearest second)
Amount
Currency
Local currency amount
Merchant category
Card issuer ID
ATM ID
POS type
Cheque account prefix
Savings account prefix

Acquiring institution ID
Transaction authorisation code
Online authorisation performed
New card
Transaction exceeds floor limit
Number of times chip has been accessed
Merchant city name
Chip terminal capability
Chip card verification result

............
A commercial example:

US Patent 5,819,226 (see USPTO website) on *Fraud detection and modeling*, (HNC Software in 1992) lists the following variables:

Customer usage pattern profiles representing time-of-day and day-of-week profiles;
Expiration date for the credit card;
Dollar amount spent in each SIC (Standard Industrial Classification) merchant group category during the current day;
Percentage of dollars spent by a customer in each SIC merchant group category during the current day;
Number of transactions in each SIC merchant group category during the current day;
Percentage of number of transactions in each SIC merchant group category during the current day;
Categorization of SIC merchant group categories by fraud rate (high, medium, or low risk);
Categorization of SIC merchant group categories by customer types (groups of customers that most frequently use certain SIC categories);
Categorization of geographic regions by fraud rate (high, medium, or low risk);
Categorization of geographic regions by customer types;
Mean number of days between transactions;
Variance of number of days between transactions;
Mean time between transactions in one day;
Variance of time between transactions in one day;
Number of multiple transaction declines at same merchant;
Number of out-of-state transactions;
Mean number of transaction declines;
Year-to-date high balance;
Transaction amount;
Transaction date and time;
Transaction type.
“Additional fraud-related variables which may also be considered are listed below”
profile total dollars of approvals in a month ptdau profile total dollars of auths in a month ptdau dy profile total dollars of auths in a day ptdcsapv profile total dollars of transactions in SIC factor group 01 ptdcsfa02 profile total dollars of transactions in SIC factor group 02 ptdcsfa03 profile total dollars of transactions in SIC factor group 03 ptdcsfa04 profile total dollars of transactions in SIC factor group 04 ptdcsfa05 profile total dollars of transactions in SIC factor group 05 ptdcsfa06 profile total dollars of transactions in SIC factor group 06 ptdcsfa07 profile total dollars of transactions in SIC factor group 07 ptdcsfa08 profile total dollars of transactions in SIC factor group 08 ptdcsfa09 profile total dollars of transactions in SIC factor group 09 ptdcsfa10 profile total dollars of transactions in SIC factor group 10 ptdcsfa11 profile total dollars of transactions in SIC factor group 11 ptdcsfa01 profile total dollars of transactions in SIC fraud rate group 01 ptdcsfa02 profile total dollars of transactions in SIC fraud rate group 02 ptdcsfa03 profile total dollars of transactions in SIC fraud rate group 03 ptdcsfa04 profile total dollars of transactions in SIC fraud rate group 04 ptdcsfa05 profile total dollars of transactions in SIC fraud rate group 05 ptdcsfa06 profile total dollars of transactions in SIC fraud rate group 06 ptdcsfa07 profile total dollars of transactions in SIC fraud rate group 07 ptdcsfa08 profile total dollars of transactions in SIC fraud rate group 08 ptdcsfa09 profile total dollars of transactions in SIC fraud rate group 09 ptdcsfa10 profile total dollars of transactions in SIC fraud rate group 10 ptdcsfa11 profile total dollars of transactions in SIC fraud rate group 11 ptdcsfa01 profile total dollars of transactions in SIC fraud rate group 01 ptdcsfa02 profile total dollars of transactions in SIC fraud rate group 02 ptdcsfa03 profile total dollars of transactions in SIC fraud rate group 03 ptdcsfa04 profile total dollars of transactions in SIC fraud rate group 04 ptdcsfa05 profile total dollars of transactions in SIC fraud rate group 05 ptdcsfa06 profile total dollars of transactions in SIC fraud rate group 06 ptdcsfa07 profile total dollars of transactions in SIC fraud rate group 07 ptdcsfa08 profile total dollars of transactions in SIC fraud rate group 08 ptdcsfa09 profile total dollars of transactions in SIC fraud rate group 09 ptdcsfa10 profile total dollars of transactions in SIC fraud rate group 10 ptdcsfa11 profile total dollars of transactions in SIC fraud rate group 11 ptdcsfa01 profile total dollars of transactions in SIC fraud rate group 01 ptdcsfa02 profile total dollars of transactions in SIC fraud rate group 02 ptdcsfa03 profile total dollars of transactions in SIC fraud rate group 03 ptdcsfa04 profile total dollars of transactions in SIC fraud rate group 04 ptdcsfa05 profile total dollars of transactions in SIC fraud rate group 05 ptdcsfa06 profile total dollars of transactions in SIC fraud rate group 06 ptdcsfa07 profile total dollars of transactions in SIC fraud rate group 07 ptdcsfa08 profile total dollars of transactions in SIC fraud rate group 08 ptdcsfa09 profile total dollars of transactions in SIC fraud rate group 09 ptdcsfa10 profile total dollars of transactions in SIC fraud rate group 10 ptdcsfa11 profile total dollars of transactions in SIC fraud rate group 11

Imperial College
London

Société Française de Statistique
Unbalanced classes

Detector correctly identifies 99 in 100 legitimate transactions and correctly identifies 99 in 100 fraudulent transactions

Pretty good?

But if only 1 in 1000 transactions are fraudulent?
<table>
<thead>
<tr>
<th>Predicted class</th>
<th>True class</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Legit</td>
</tr>
<tr>
<td>Legit</td>
<td>99%</td>
</tr>
<tr>
<td>Fraud</td>
<td>1%</td>
</tr>
</tbody>
</table>

**Numbers**

|  |  
|---|---|
| 999 | 1 |
91% of suspected frauds are in fact legitimate

This matters because:

- operational decisions must be made (stop card?)
- good customers must not be irritated

Customers are pleased you care: up to a point
Delay in learning class labels

- if fraud alarm is raised, then true class quickly known
- if no alarm, then not detected until statement

This makes it different from the standard supervised classification paradigm

Banks cannot always say when a fraud commences
Mislabelled classes

Not all fraudulent transactions are labelled as fraud (account holder fails to check carefully)

Not all legitimate transactions are labelled as legitimate

Subtlety: account holder makes transactions and then claims card was stolen

Such transactions are fraudulent because the holder declares them as such
Reactive population drift

- banks implement detection/prevention strategies

- fraudsters don’t generally give up!
  - but change their strategies
Reactive population drift example: *Chip and PIN*

*Chip and PIN intended/predicted to end card fraud*

After UK rollout on 14 Feb 06, UK CC fraud declined

How much was a consequence of the publicity?

*but*

- Lloyds TSB observed increase in fraudulent use of UK cards in Europe (no C&P – mag stripe counterfeited)

- observed increase in ATM and cardholder not present fraud
Plastic card fraud in the UK

The waterbed effect

Source: APACS

Card not present
Counterfeit
Lost stolen
Card ID theft
Mail non receipt
What is a good system?

‘Classifies fraudulent transactions as fraudulent, and legitimate transactions as legitimate’?

But: no method is perfect
Need: criteria for assessing effectiveness
Timeliness: time scale: count of fraud transactions misclassified
Different weights on two kinds of misclassification
Overall performance measure for given threshold:

\[ T_1 = \left( a + b + kc \right) / \left( ka + kc + b + d \right) \]

where \( k \) is the estimated relative cost of misclassifying a fraud as legitimate compared to misclassifying a legitimate as fraud.

Or, if the bank can afford to investigate \( C \) cases

\[ T_2 : \text{minimise } c \text{ subject to } \left( a + b \right) = C \]
Constructing detectors

Core approaches:
  • rule-based methods
  • supervised classification
  • anomaly detection

  • change point detection
  • multilevel methods (transaction/account/merchant)
  • link analysis - networks

Activity records
Different approaches have different merits

rule-based:
- need expert knowledge of past fraud behaviour
- highly effective at detecting known fraud types
- ineffective at novel types

supervised methods:
- need examples of past fraud
- can be effective at detecting similar occurrences
- ineffective at novel types

anomaly detection:
- good for new kinds of deviations (but behaviour may change)
- not good for known types
Rule-based methods

Rules from expert knowledge:
- two near simultaneous transactions using the same card at geographically dispersed locations
- small time between attempts to withdraw maximum amount
- excessively small transactions
- multiple small electrical items
- ....
**Supervised classification**

Basic principle:

Given a set of known fraudulent and legitimate transactions/accounts,

along with descriptive variables for each,

condense these to a rule enabling correct classification of new transactions/accounts

using only their descriptive variables
Example:

- 175 million transactions: 1st August 05 to 30th Nov 05
- 16.8 million accounts
- 5,946 accounts with fraud at POS terminals
- 76 raw variables per transaction; mostly categorical

- rolling window activity records - 0, 1, 3, 7 days
- activity records $\Rightarrow$ 87 variables per transaction
Performance of models on independent test set
Outliers

Basic principle: build a model for the ‘norm’ for this customer and detect when it deviates

‘Norm’ can be based on
- this customer compared with self at previous times (jamjarring)
- this customer compared with other customers
- life stage card usage patterns
- segmentation into customer types
- a combination of these

Basic advantage of one-class approach
- can detect new kinds of anomalies, not seen before
- more power in dynamic fraud environment?
Example:

- 44,637 accounts
- 2,374,311 transactions
- 3,742 fraudulent accounts
- 53,844 fraudulent transactions
- 3 months data

77 raw variables, from which we used

- size of transaction
- difference between current and previous transaction size
- sum of current and previous transaction sizes
- product of current and previous transaction sizes
- time of transaction
- time between current and previous transaction
- merchant category code (MCC)
- ATM ID code
Inliers: Peer group analysis

Individual account profiles:
Model behaviour and compare new transaction with past

But
Spending behaviour just before Christmas is anomalous
Individual profile models may flag such transactions

So
Identify others with similar past behaviour (peer group)
Compare new transaction with their new transactions
Target account tracks peer group
Change point detection

e.g. (mean time between alarms prior to change) / (mean time between alarms after change)

ATM Transactions over time
Cumulative CC spend in gas stations

Random effects model for the compound multivariate point process
Adaptive methods

![Graph showing AUC over months for different QDA methods: Static, Streaming, Retrained.]}
**Link analysis**

*Between people:* Fraudsters don’t work in isolation (e.g. credit cards stolen or cloned and passed on). Networks.

*Between fraud types:* a gang which carries out one kind of fraud probably also carries out others.

Networks
Data fusion

“Fraud management requires a holistic approach, blending tactical and strategic solutions with the state-of-the-art technology solutions and best practice in fraud strategy and operations”

James Gilmour, Editor Credit Risk International, 2003
Conclusions

Fraud detection problems

- large data sets
- messy data
- unbalanced classes
- may have mislabelled classes
- delay in labelling
- dynamic, reactive data distributions
Other, deeper questions

Is society changing, and accepting some degree of fraud?

Letter from London Times, August 13, 2007

“Sir, I was recently the victim of an internet fraud. The sum involved was several hundred pounds. My local police refused to investigate, stating that their policy was to investigate only for sums over £5000.”
Like the poor, fraud is always with us
END

d.j.hand@imperial.ac.uk