Transaction Fraud Scoring

John Oxley

John.Oxley@uk.experian.com

Credit Scoring and Credit Control IX, Edinburgh 2005

Agenda

- Introduction
  - Credit card fraud losses and types of fraud
  - Authorisation and transaction flow
- Prevention and detection
  - Chip and PIN
  - Biometrics
  - Rule based system
  - Transaction fraud scoring
- Modelling process
  - Sample
  - Methodology
- Performance
  - % frauds detected
  - FPR etc.
- Score Implementation
  - Implementation mode
  - Preparation
- Monitoring
  - Performance degradation
  - Updating the model

Fraud losses

- Total Losses on UK issued cards in 2004:

£504.8m

20% increase on 2003

- Organised crime activity pre Chip and PIN

- Total Losses on UK issued credit cards due to Bad Debt in 2004:

£1,601m

- Fraud linked to organised crime and terrorism

Source: APACS, Bank of England

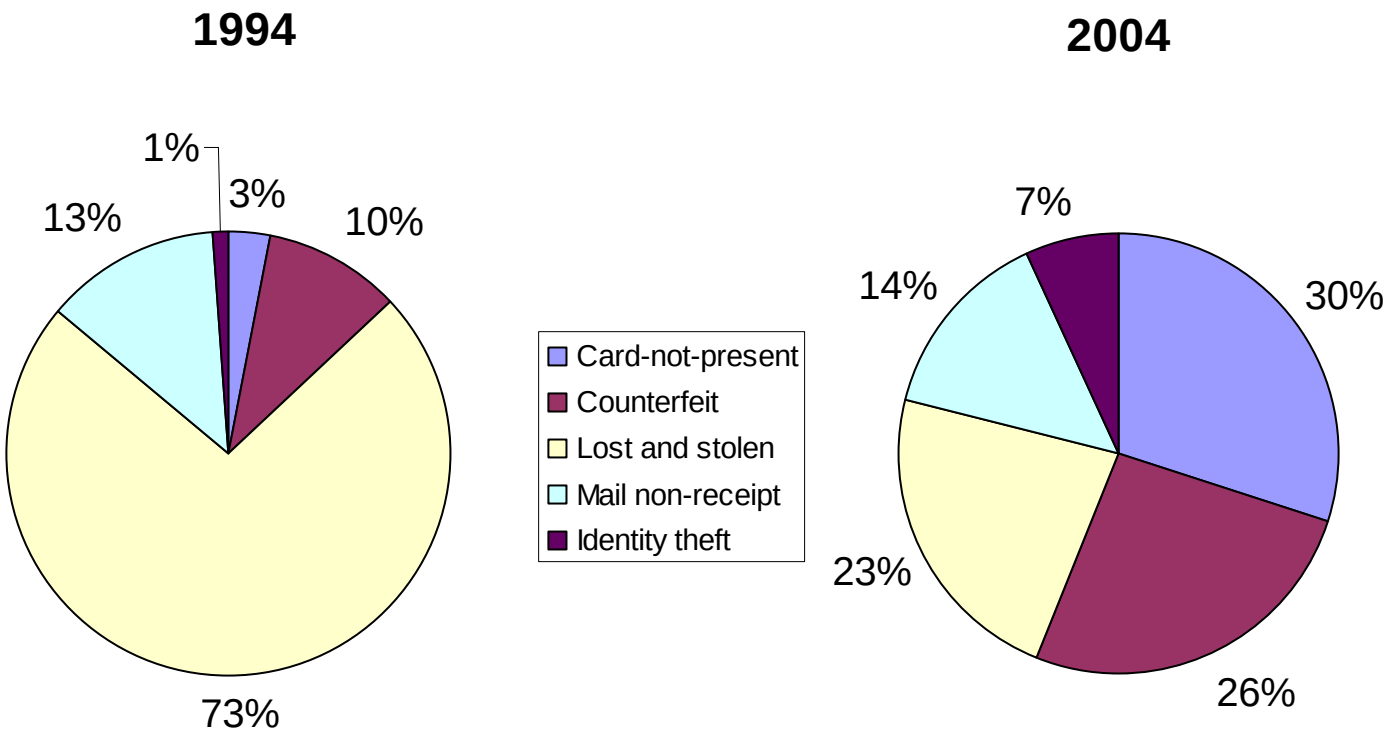
Fraud characteristics

- International organised crime
- Rapidly changing methods
  - Shoulder surfing
  - ‘Lebanese loop’
  - Skimming
  - Bin raiding
  - Bust out/sleeper fraud
  - Corrupt staff
- Technologically advanced
  - Fraudsters IT literate
  - Wire tapping
  - Hand held card readers
  - Phishing

Fraud types

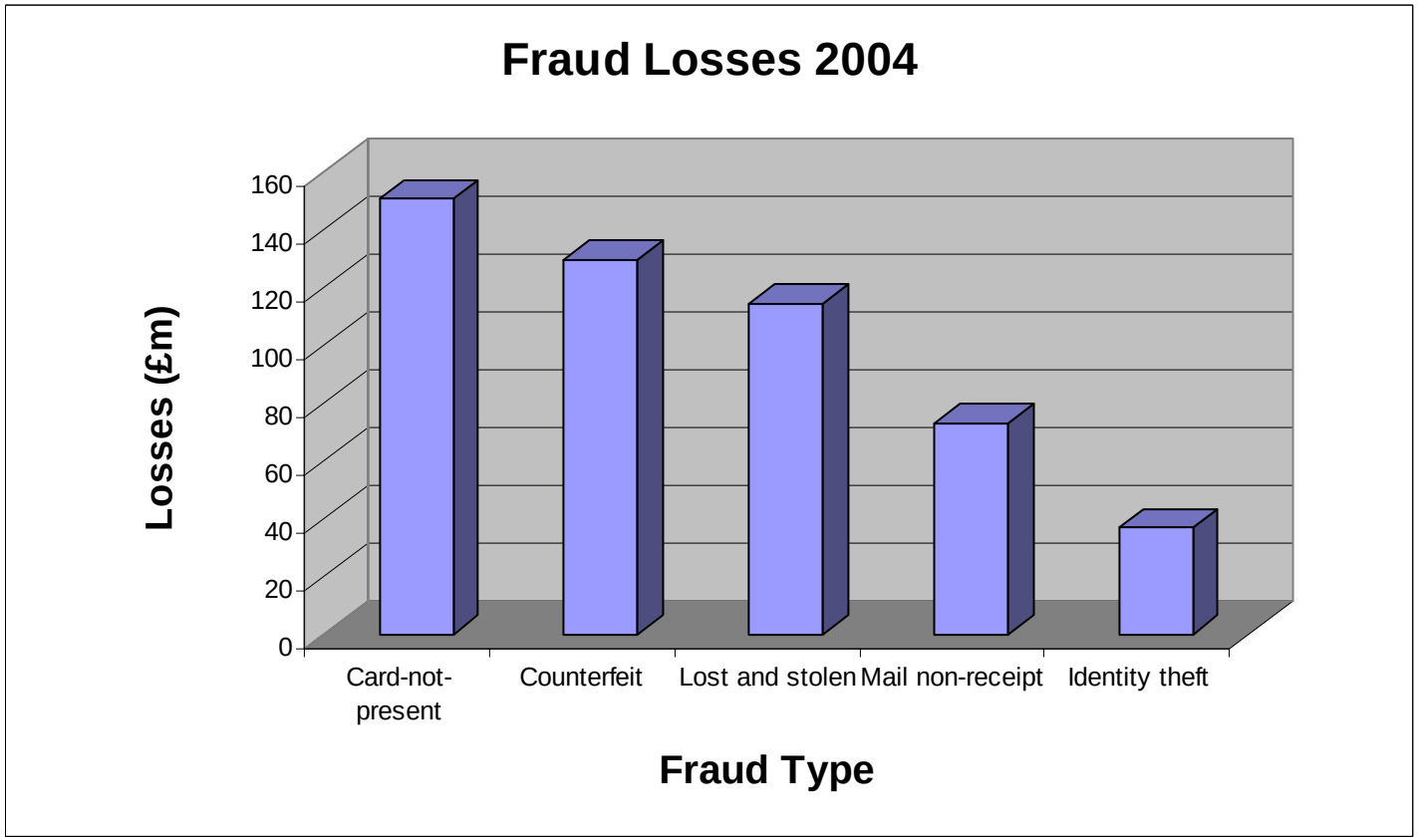
- Lost/stolen
  - Cards that have been reported by the cardholder as lost or stolen
- Counterfeit
  - A counterfeit, cloned or skimmed card is one that has been printed, embossed or encoded without permission from the card company or one that has been validly issued and then altered or recoded. Also Computer generated card numbers, collusion, wire tapping
- Mail non-receipt
  - Cards stolen in transit - after card companies send them out and before the genuine cardholders receive them
- Card not present
  - Usually the theft of genuine card details that are then used to make a purchase through a remote channel such as the phone, Internet, fax or mail order.
- Identity fraud
  - A criminal uses fraudulently obtained personal information to open or access card accounts in someone else's name. Perpetrated through Application fraud and Account takeover.

Changing patterns of fraud – UK issued cards



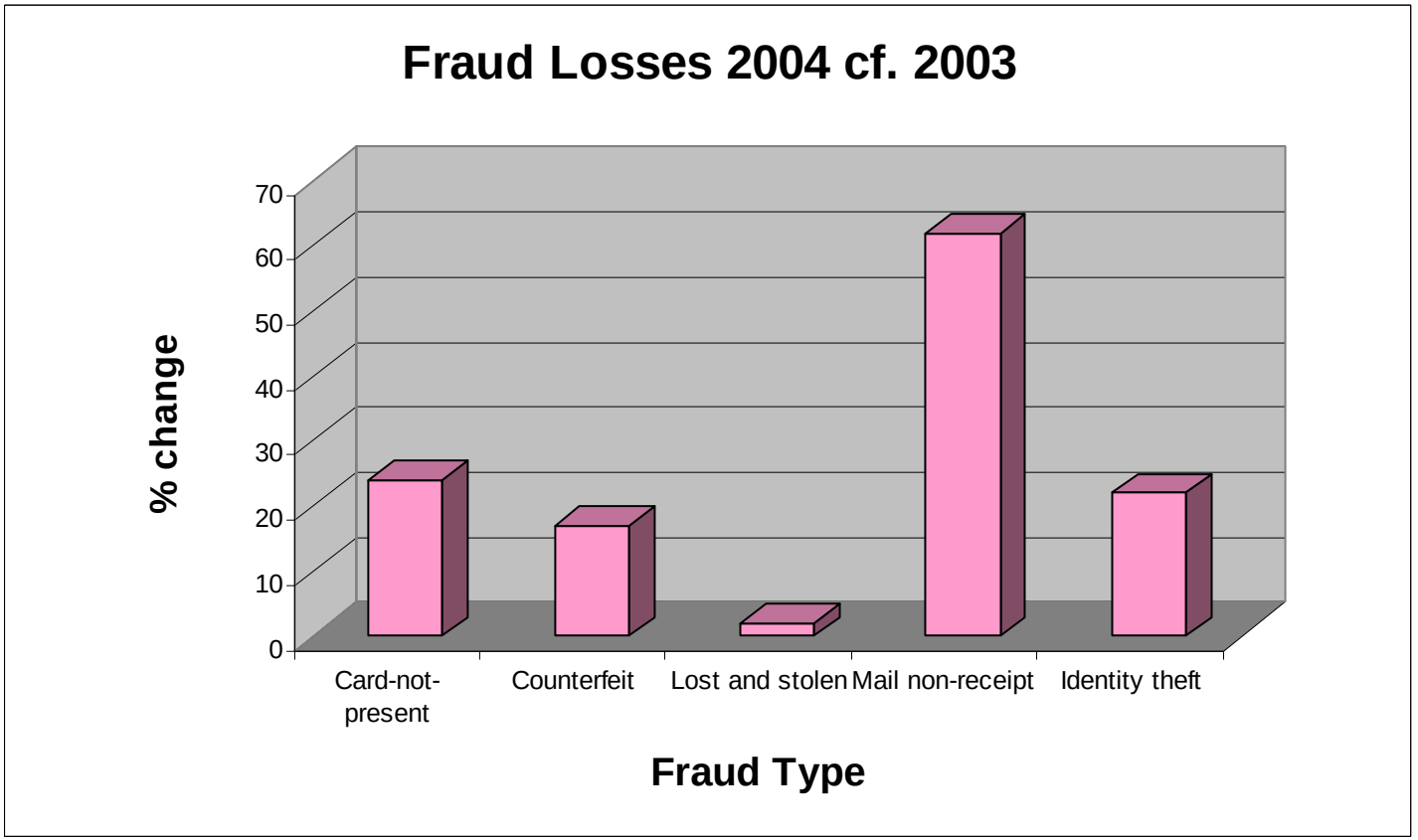
Source: APACS

Fraud losses – UK issued cards



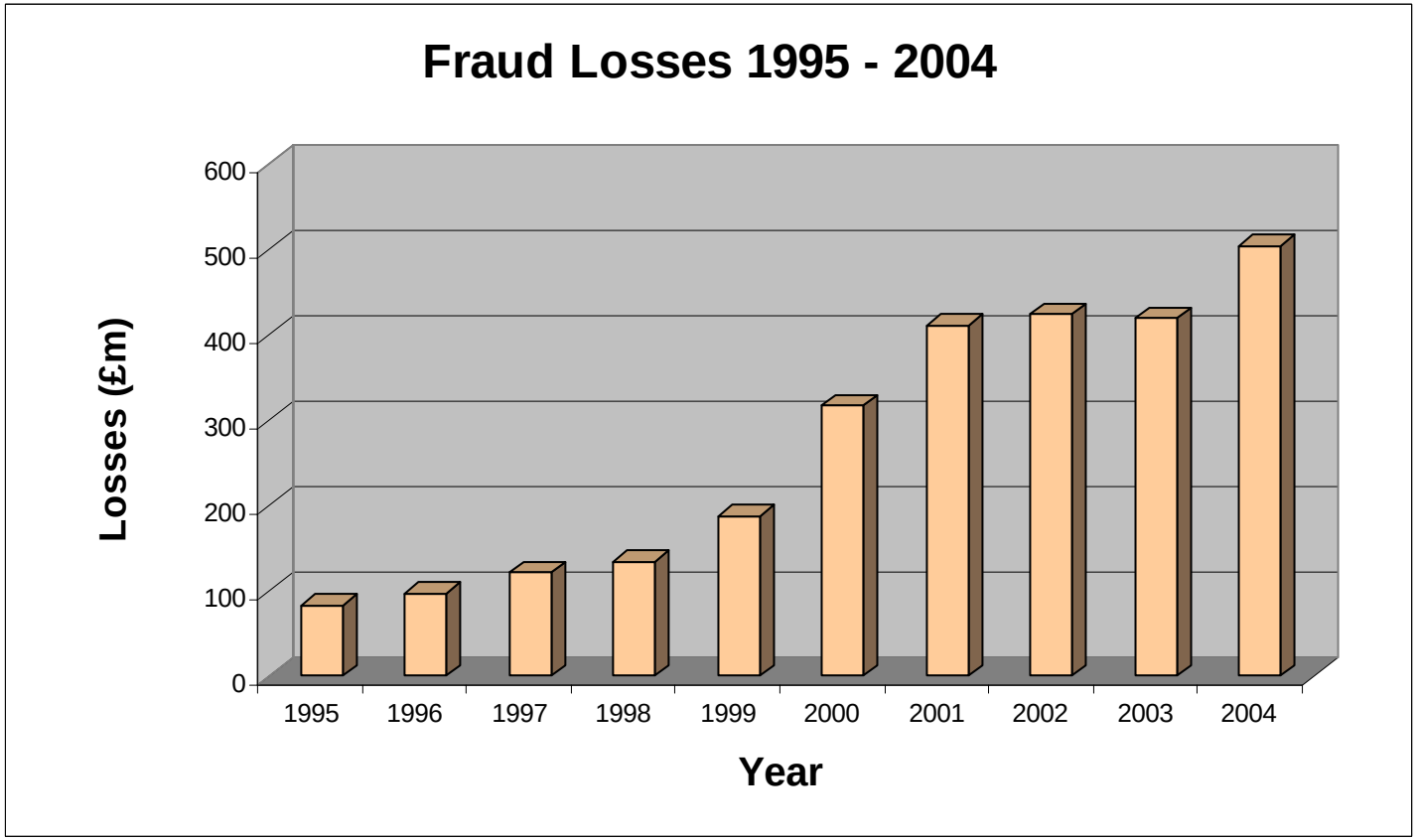
Source: APACS

Fraud losses – UK issued cards



Source: APACS

Fraud losses – UK issued cards



Source: APACS

Extent of fraud – UK issued cards

- Losses against turnover 2004 0.141%
- Losses against turnover 2003 0.135%
- Peak in 1991: 0.33%

Source: APACS

Agenda

- Introduction
  - Credit card fraud losses and types of fraud
  - Authorisation and transaction flow
- Prevention and detection
  - Chip and PIN
  - Biometrics
  - Rule based system
  - Transaction fraud scoring
- Modelling process
  - Sample
  - Methodology
- Performance
  - % frauds detected
  - FPR etc.
- Score Implementation
  - Implementation mode
  - Preparation
- Monitoring
  - Performance degradation
  - Updating the model

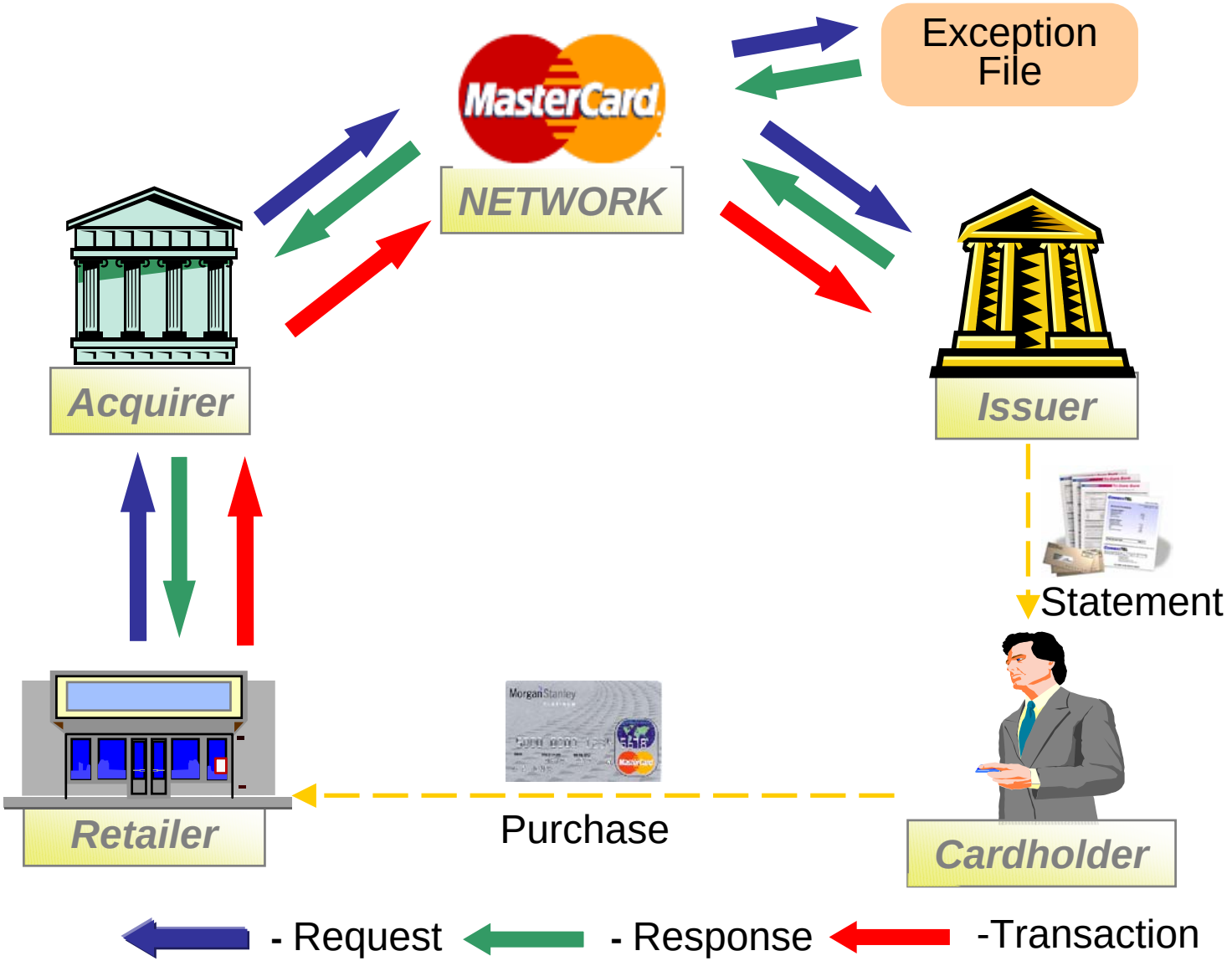
Fraud prevention

- Verification and validation
  - The card is genuine
  - The cardholder is the rightful owner
- Chip and PIN
  - A chip (‘smart’) card holds encrypted details on a secure microchip that can store and process information. The PIN replaces the signature for card present transactions
- Biometrics
  - Methods of identification by measuring unique human characteristics as a way to confirm identity. Examples are finger or iris scanning or dynamic signature verification
- Card Security Code (CSC)
  - The last three or four digits of a number (formerly CV2) printed on or just below the signature panel on payment cards. It can be requested for CNP transactions in addition to card expiry date etc.
- Other features
  - Holograms, UV, unique fonts

The need for transaction fraud detection

- Around 10% of cardholders keep their PIN with their card
- Fraud migration
- Staff collusion
- Merchant collusion
- Increasing sophistication of fraudsters
- Chip and PIN not yet applicable to CNP transactions

Authorisation and transaction flow

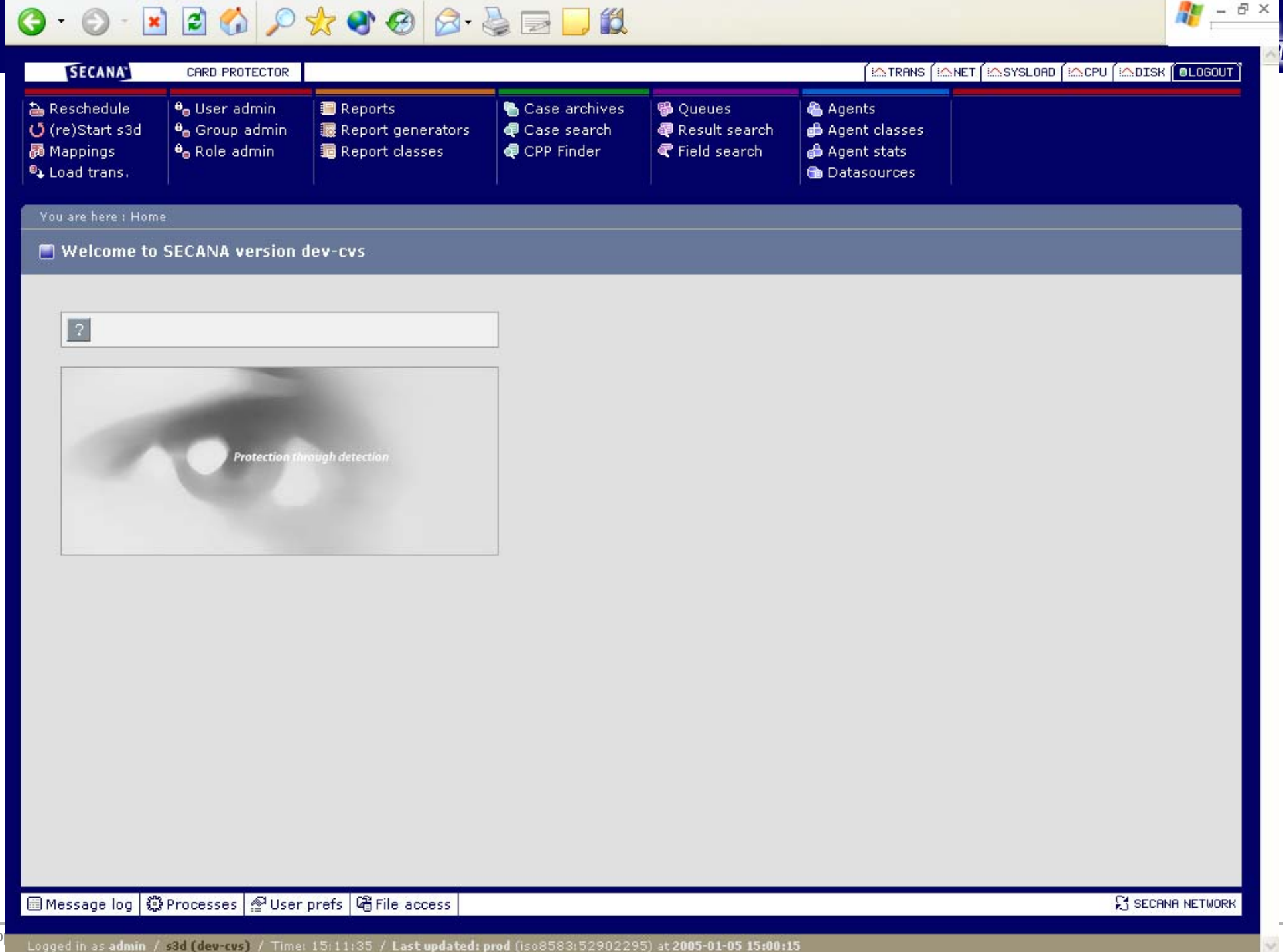


Fraud detection

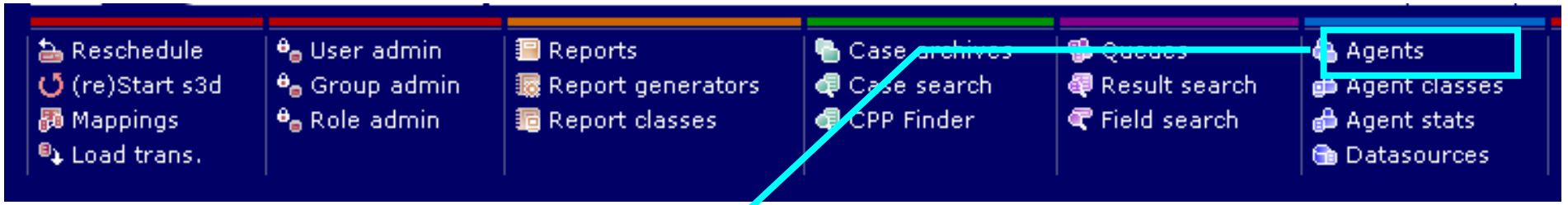
- A transactional risk management system requires the capability to
  - detect fraud at the point of sale: authorisations
  - predict trends
  - assist in investigations
  - cope with new trends
- Rule based system
- Transaction fraud score

Fraud detection

- Rule based system
  - Relatively easy to use and maintain
  - Requires a logical and comprehensive work-flow system
  - Requires ability to load different types of data
  - Generally reactive
  - Example: Secana Card Protector


SECANA
CARD PROTECTOR
TRANS
NET
SYSLOAD
CPU
DISK
LOGOUT
Reschedule
(re)Start s3d
Mappings
Load trans.
User admin
Group admin
Role admin
Reports
Report generators
Report classes
Case archives
Case search
CPP Finder
Queues
Result search
Field search
Agents
Agent classes
Agent stats
Datasources
You are here : Home
Welcome to SECANA version dev-cvs
Protection through detection
Message log
Processes
User prefs
File access
SECANA NETWORK
Logged in as admin / s3d (dev-cvs) / Time: 15:11:35 / Last updated: prod (iso8583:52902295) at 2005-01-05 15:00:15

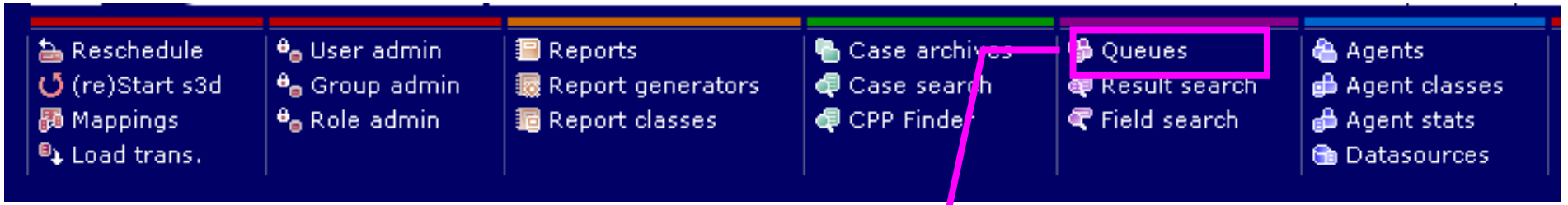
Rules based system



Datasources select the data to be used in each investigation. Grouped by cardnumber or customer

Agents are the Rules. Using input from datasources and reports they select the exception transactions – manually or automatically

Rules based system



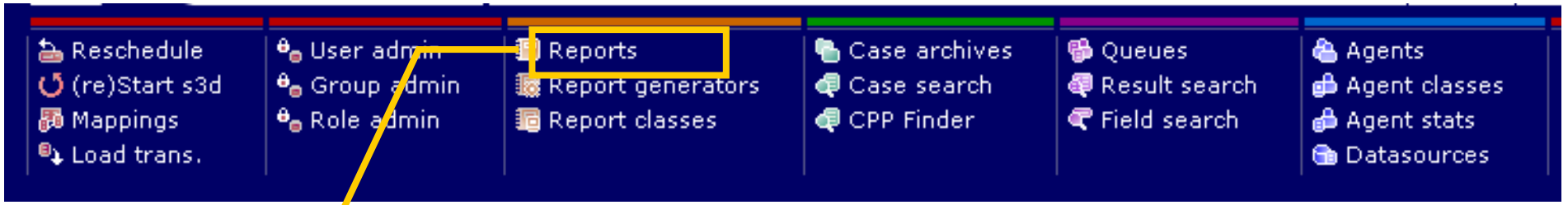
Datasources select the data to be used in each investigation. Grouped by cardnumber or customer

Agents are the Rules. Using input from datasources and reports they select the exception transactions – manually or automatically

Exceptions are placed in queues for review by case handlers

Exception issues are either checked out as OK or placed in case archives

Rules based system



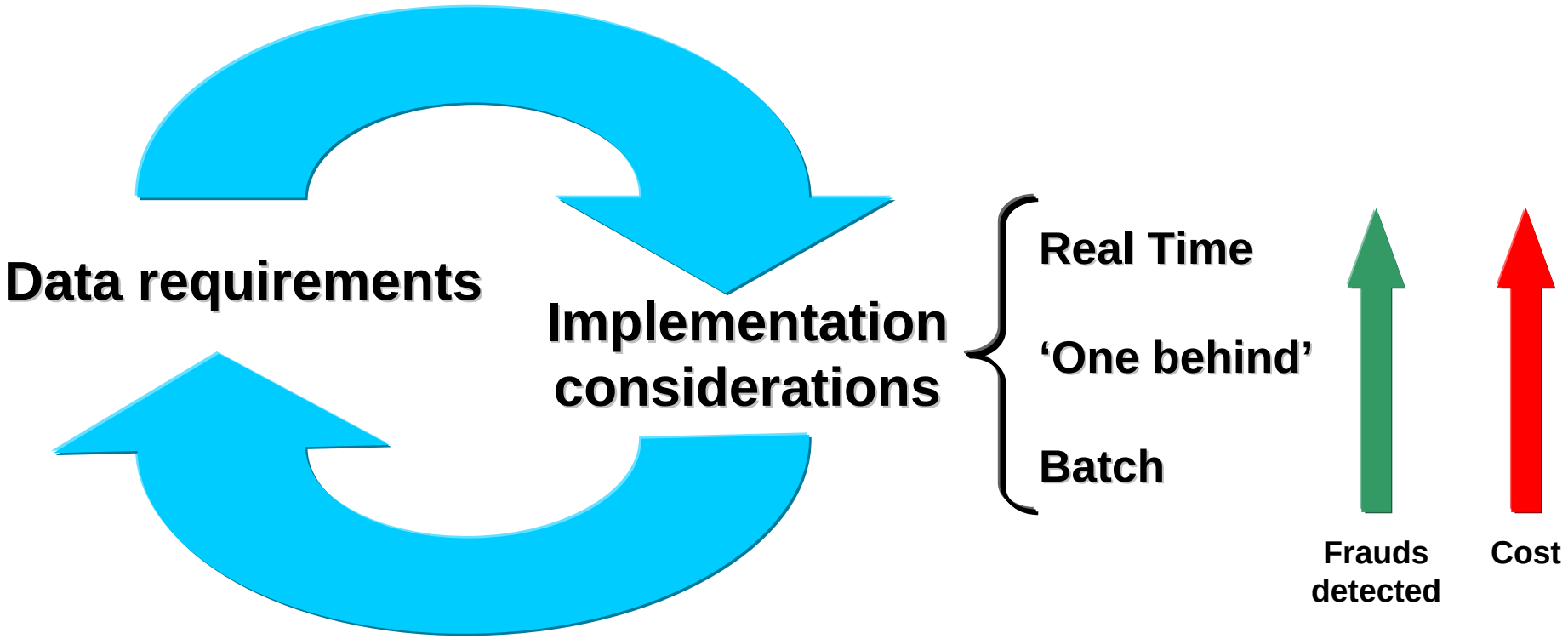
Reports

- Feed back to the agents with list of cards that have been exposed for a specific environment
- A range of management reports can be generated
  - False positive ratios
  - Success ratio for different agents
  - Performance of different operators
  - Can be mailed directly from the system
- Investigation of Common Points of Compromise (CPP)

Transaction fraud score

- Dynamic
  - Proactive – predictive characteristics may change from transaction to transaction
- Components:
  - Cardholder level profiles encapsulating normal transaction pattern
    - Frequency of use
    - Typical value range
    - Types of Goods purchased
    - Transaction types
    - Retailer profiles
    - Cash usage
    - Balance and Payment histories
    - Overseas spending patterns
    - Daily, weekly, monthly, & seasonal patterns
  - Aggregator
    - Data combined for range of time/value intervals, merchant classification
  - Score
    - Model to compare incoming transactions with the norm and known fraud indicators

Transaction fraud score



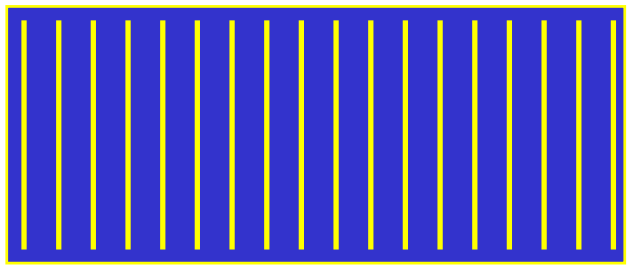
Agenda

- Introduction
  - Credit card fraud losses and types of fraud
  - Authorisation and transaction flow
- Prevention and detection
  - Chip and PIN
  - Biometrics
  - Rule based system
  - Transaction fraud scoring
- Modelling process
  - Sample
  - Methodology
- Performance
  - % frauds detected
  - FPR etc.
- Score Implementation
  - Implementation mode
  - Preparation
- Monitoring
  - Performance degradation
  - Updating the model

Modelling process

- Sample design and preparation
- Segmentation
  - Fraud types
  - Personal/company cards
  - Card types
  - Affinity scheme
  - Transaction's country of origin
  - Transaction value
- Univariate analysis and feature extraction
- Model construction with transformed predictive characteristics

Sample design – an approach



‘Observation’ period

e.g. 12+ months

Create ‘Normal transaction pattern’

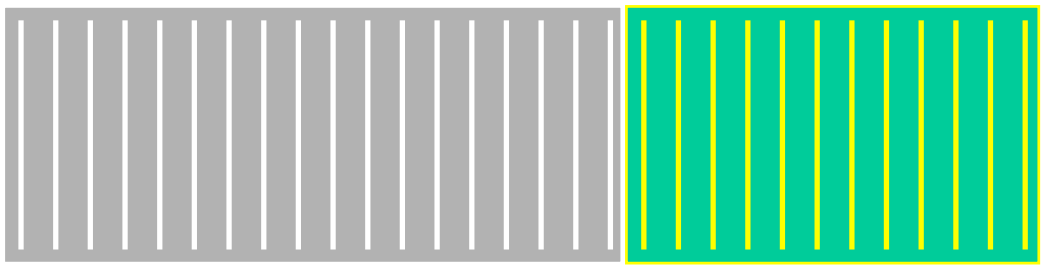
Sample design – an approach

Observation point

e.g. statement cycle point

Exclude blocked A/Cs

Create month-end snapshot



‘Observation’ period

e.g. 12+ months

Create ‘Normal transaction pattern’

‘Outcome’ period

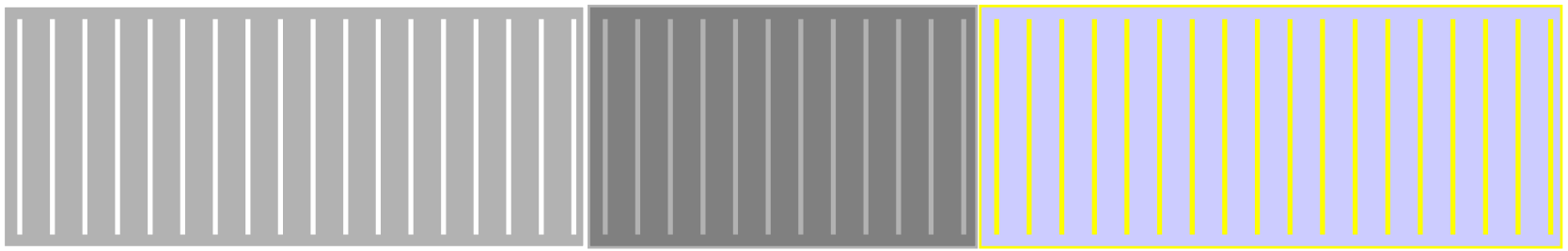
e.g. Oct statement cycle

Update certain characteristics

Sample design – an approach

Observation point

e.g. Sept statement cycle



'Observation' period

e.g. 12+ months

Post-outcome period

2-3 months

Identify 'late' fraud notification

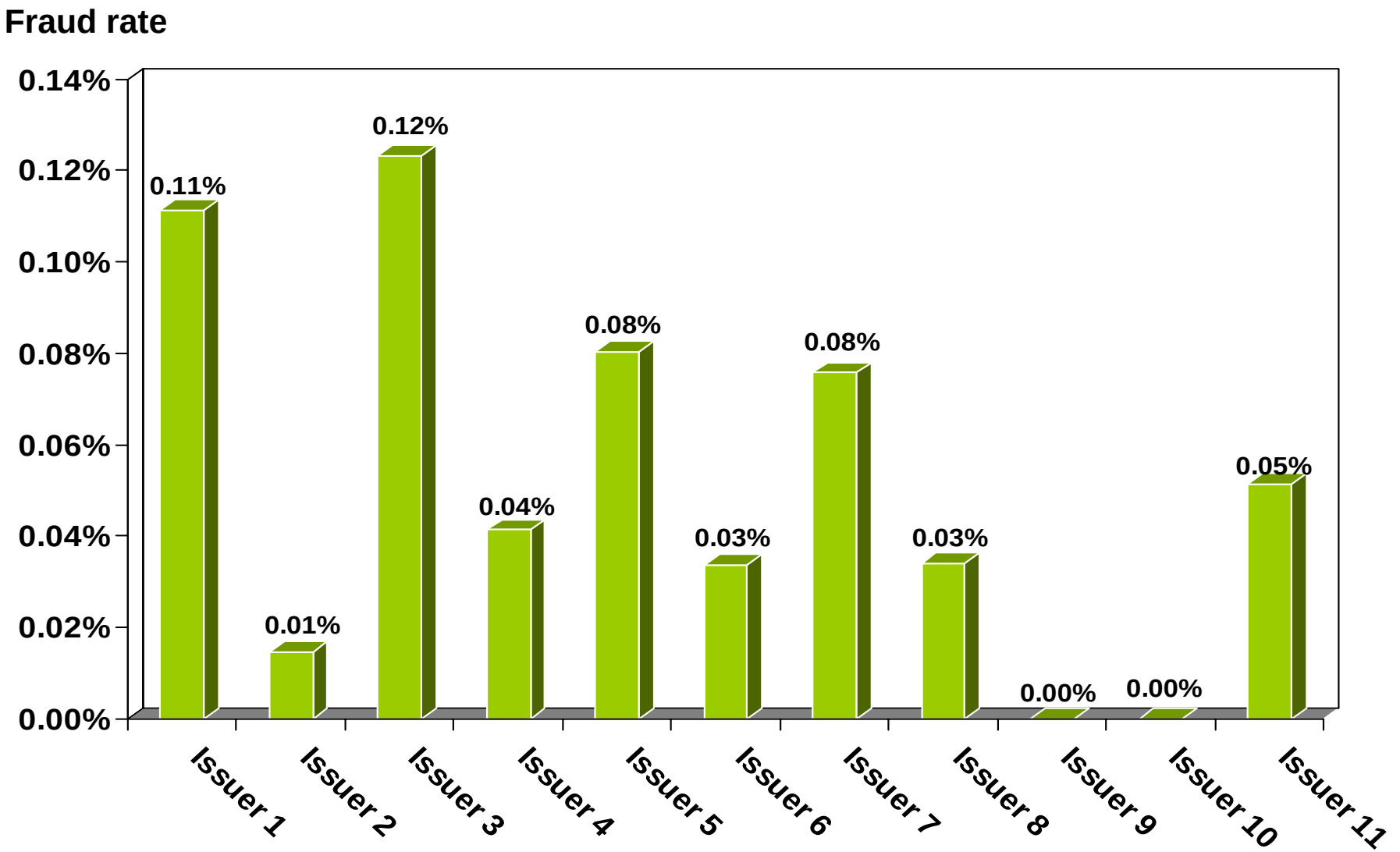
'Outcome' period

e.g. Oct statement cycle

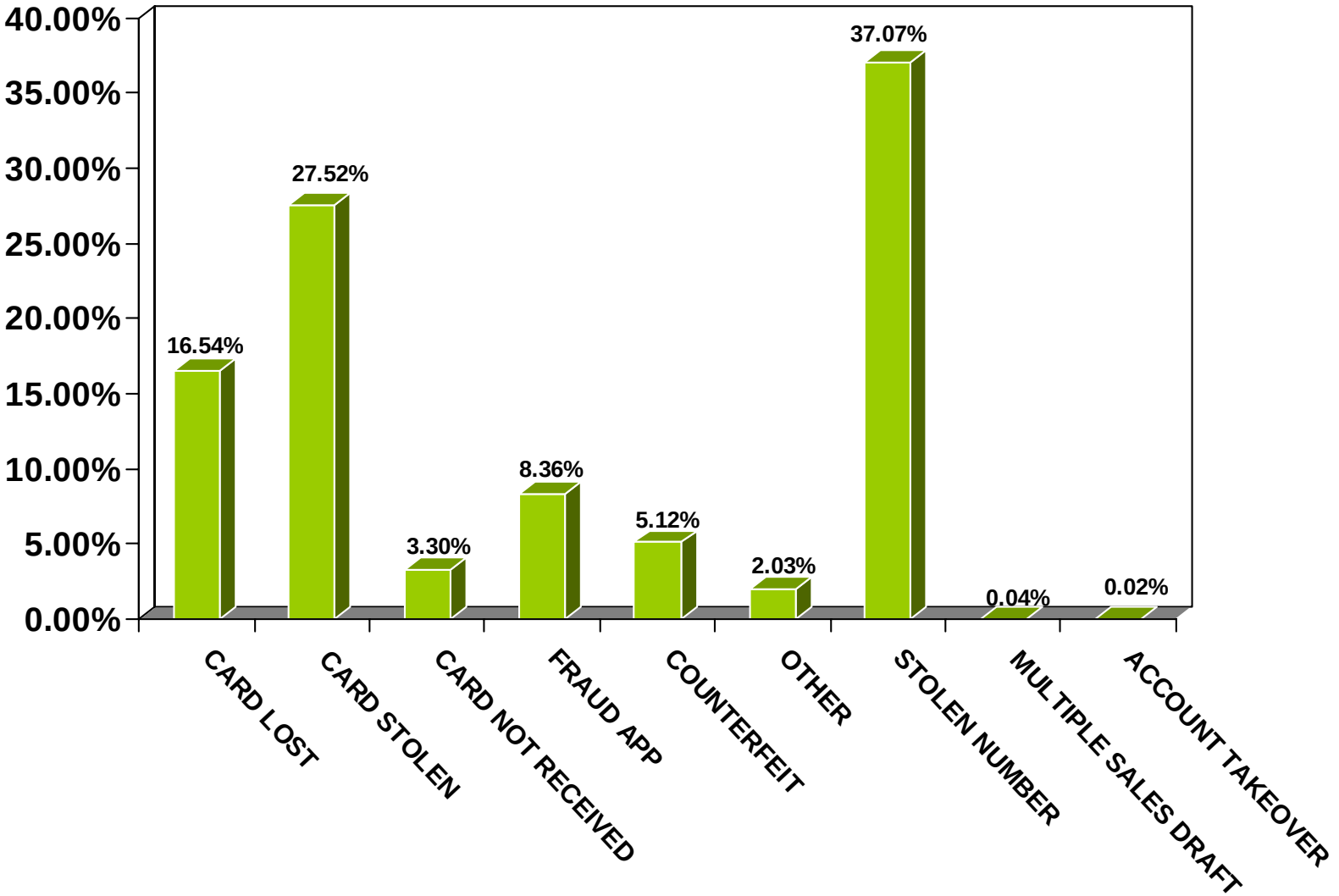
Sample design

- Data issues
  - Accurate fraud flag
  - Sufficient fraud transactions
  - Authorised and non-authorised transactions
  - Declined fraud transactions
  - Account transfer processing: refunds, disputes

US fraud sample



US fraud sample

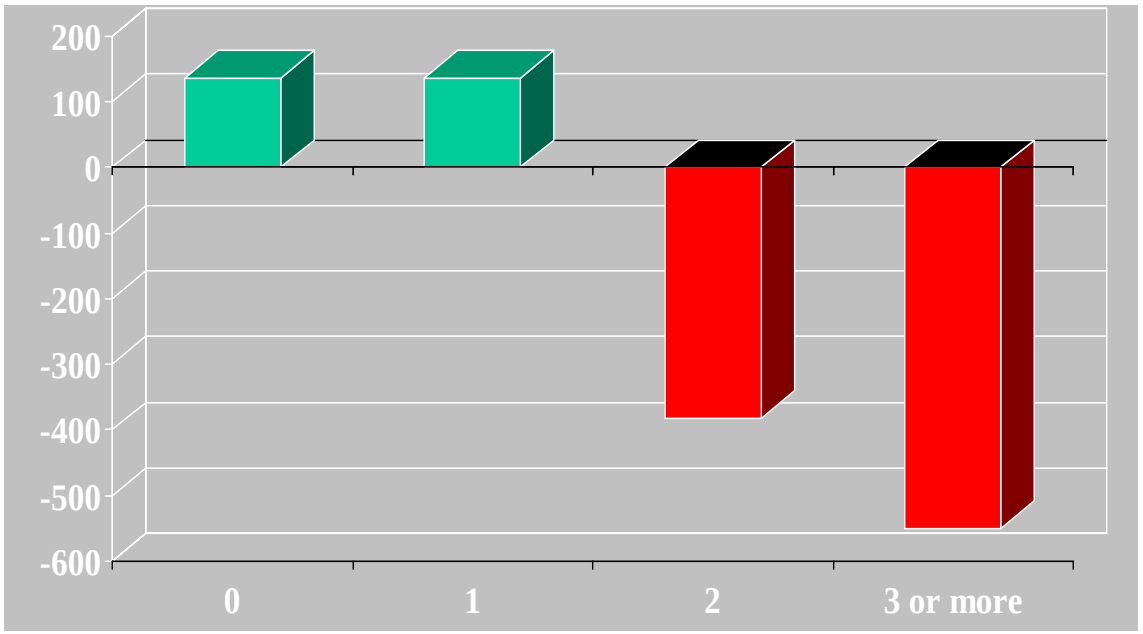


Predictive characteristic set

- Four broad categories:
  - Indices and ratings
    - E.g. Retailer fraud index, Merchandise fraud index, Transaction time index
  - Individual transaction fraud predictors
    - compare the current transaction with the normal behaviour profile
    - is the normal behaviour profile stored or calculated each time?
  - Typical fraud rules
    - E.g. accounts with more than 5 cash transactions in one day, accounts where high value transactions are taking place in a country known for fraud, accounts used to make many telephone calls in one day
  - Trigger events
    - Card issue, PIN request, change of address, overpayment, large payment

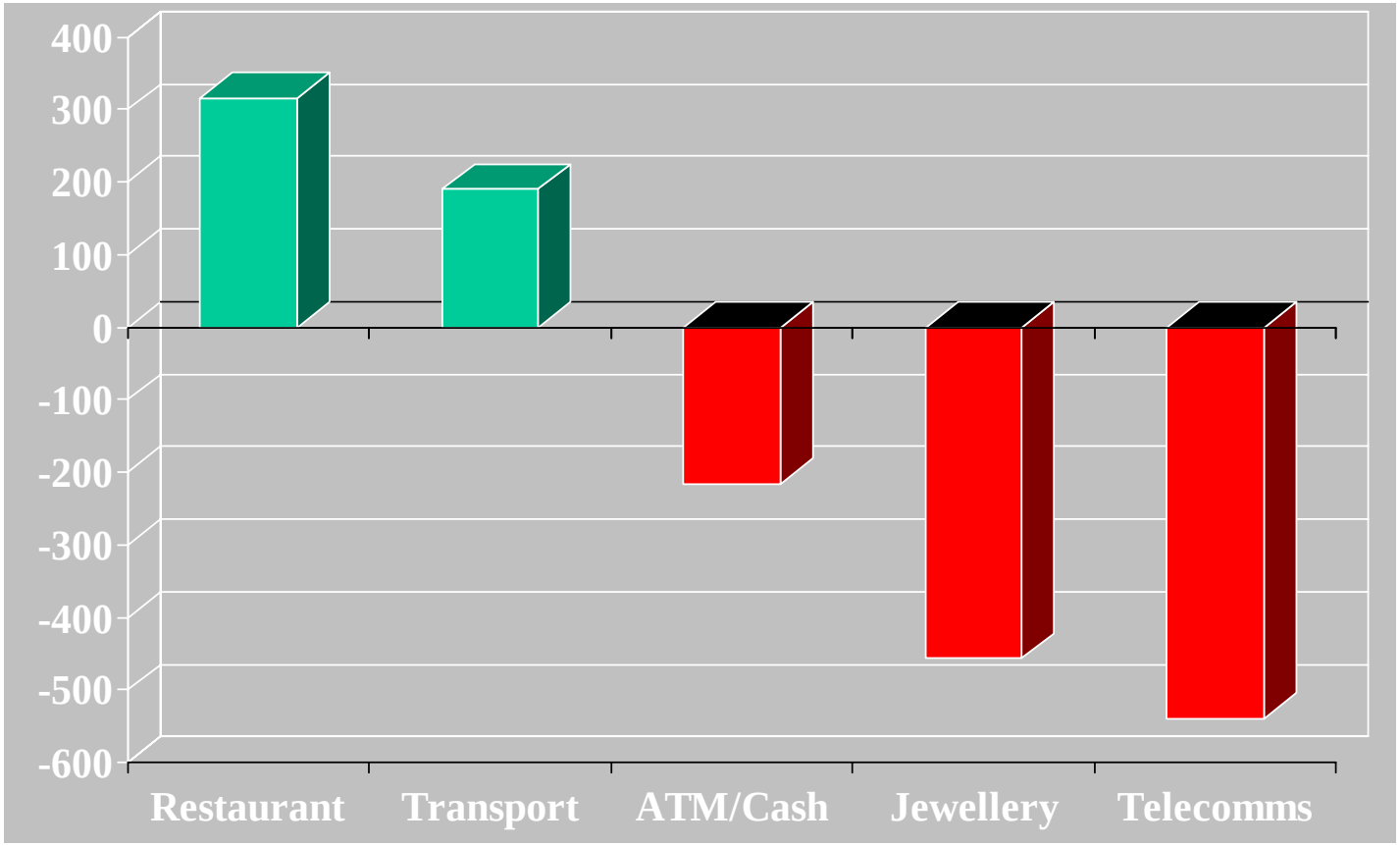
Transactions of unusual value

Good: Fraud index



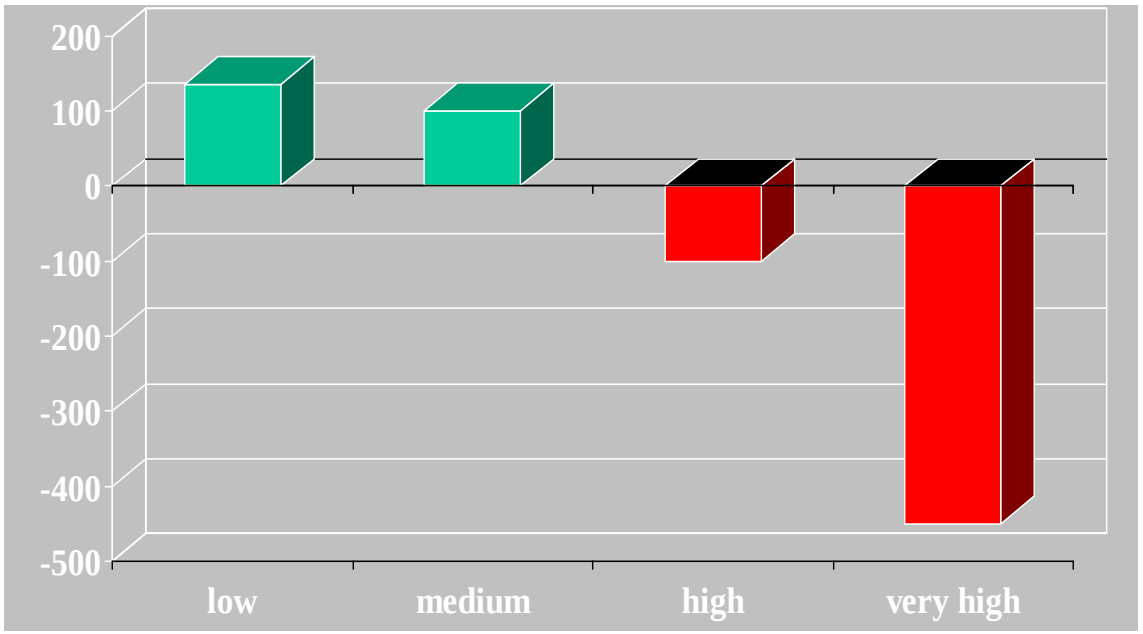
Merchant Category

Good: Fraud index

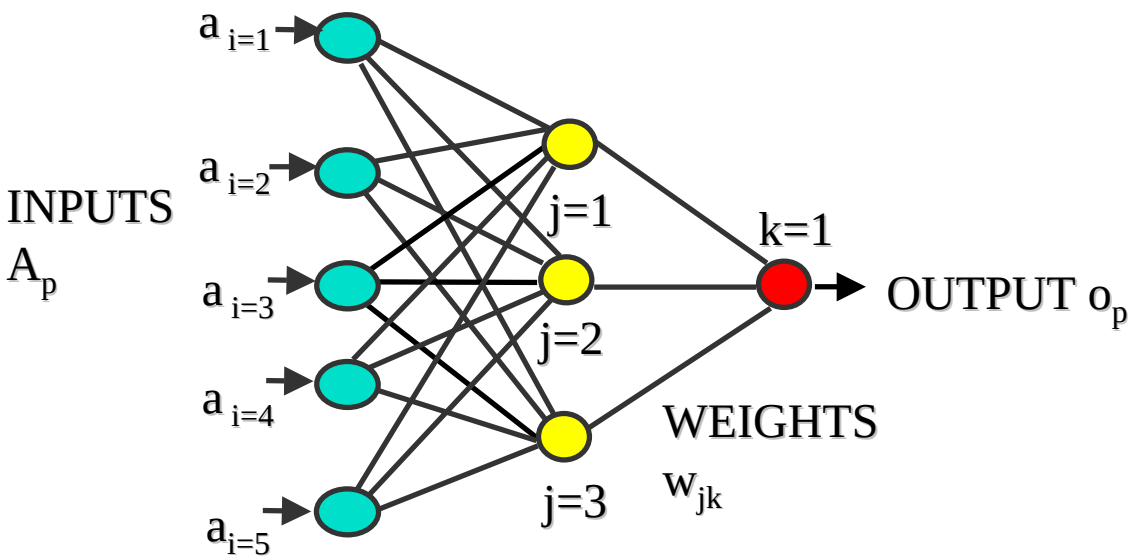


Transaction velocity cf. average

Good: Fraud index



- Artificial neural networks
  - Global approximation e.g. multilayer perceptron with backpropagation learning algorithm



  - Local approximation e.g. variants on radial basis function networks

- Regression techniques

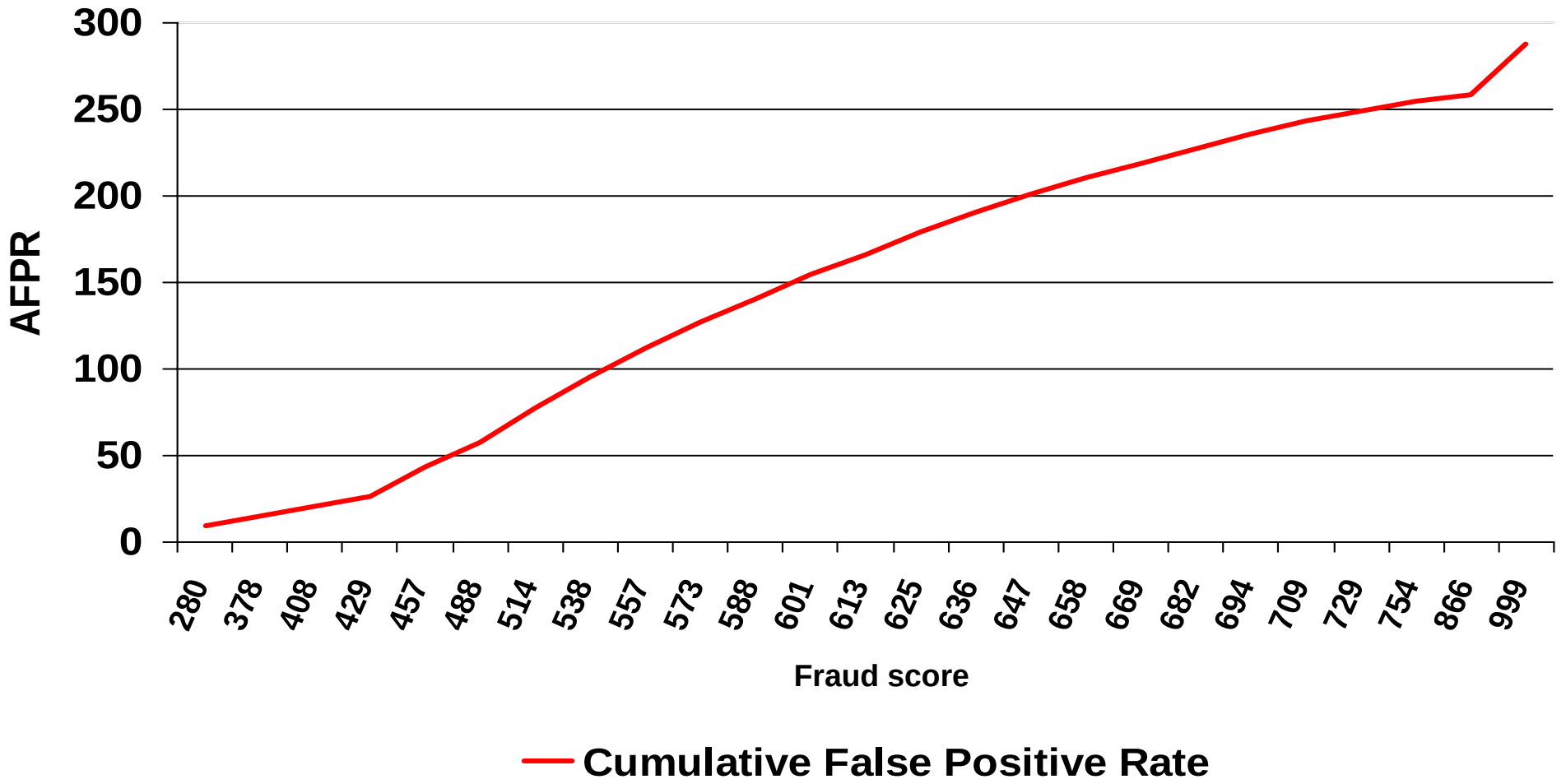
Agenda

- Introduction
  - Credit card fraud losses and types of fraud
  - Authorisation and transaction flow
- Prevention and detection
  - Chip and PIN
  - Biometrics
  - Rule based system
  - Transaction fraud scoring
- Modelling process
  - Sample
  - Methodology
- Performance
  - % frauds detected
  - FPR etc.
- Score Implementation
  - Implementation mode
  - Preparation
- Monitoring
  - Performance degradation
  - Updating the model

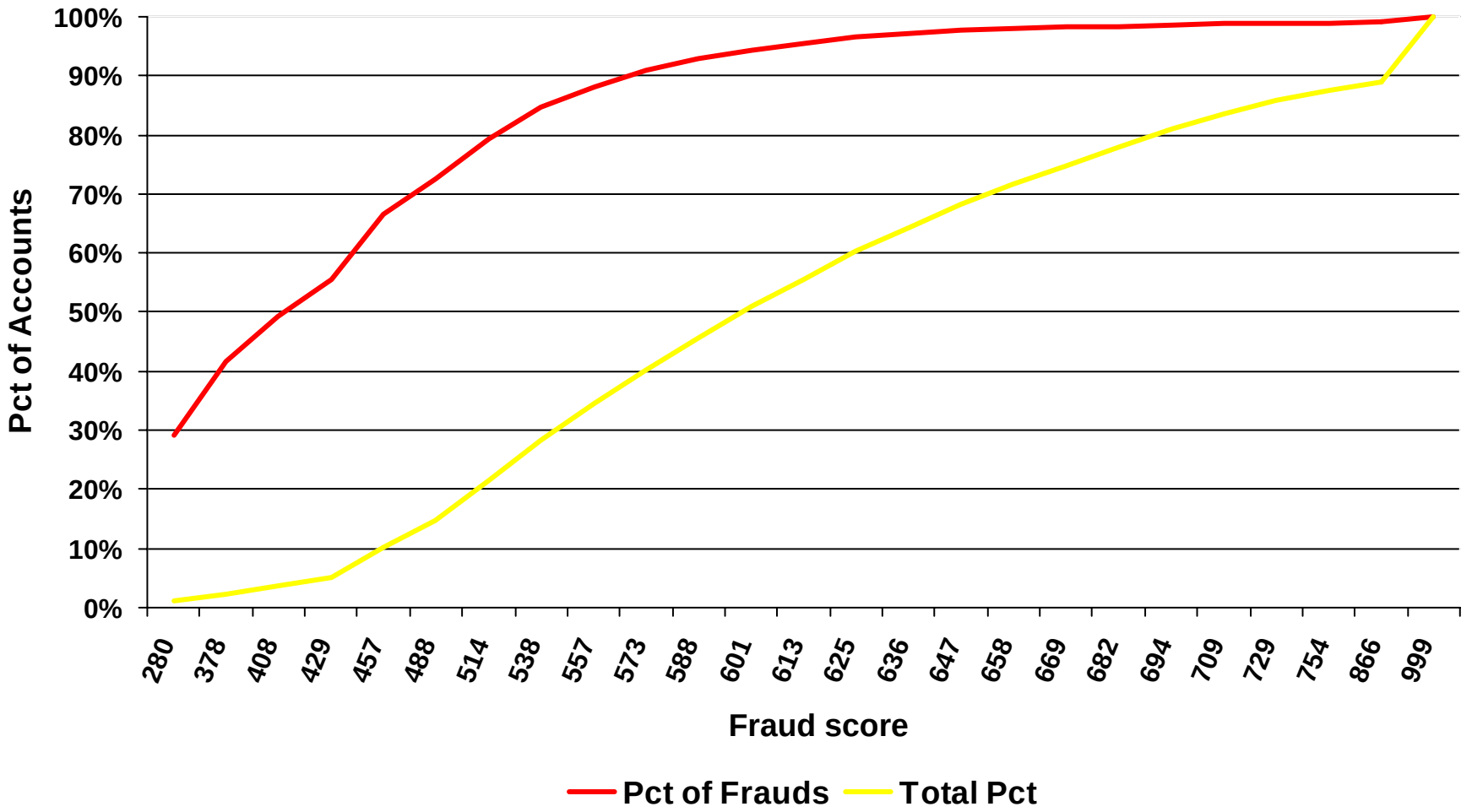
Model performance

- Development and validation samples
- For a given cut-off score
  - % Fraud transactions detected
  - False positive rate
    - transaction level and account level
    - balance fraud prevention against customer service
  - # and % of accounts referred
    - fraud investigation team typically 5-6 people
  - Value of frauds detected
  - % and value of first frauds detected

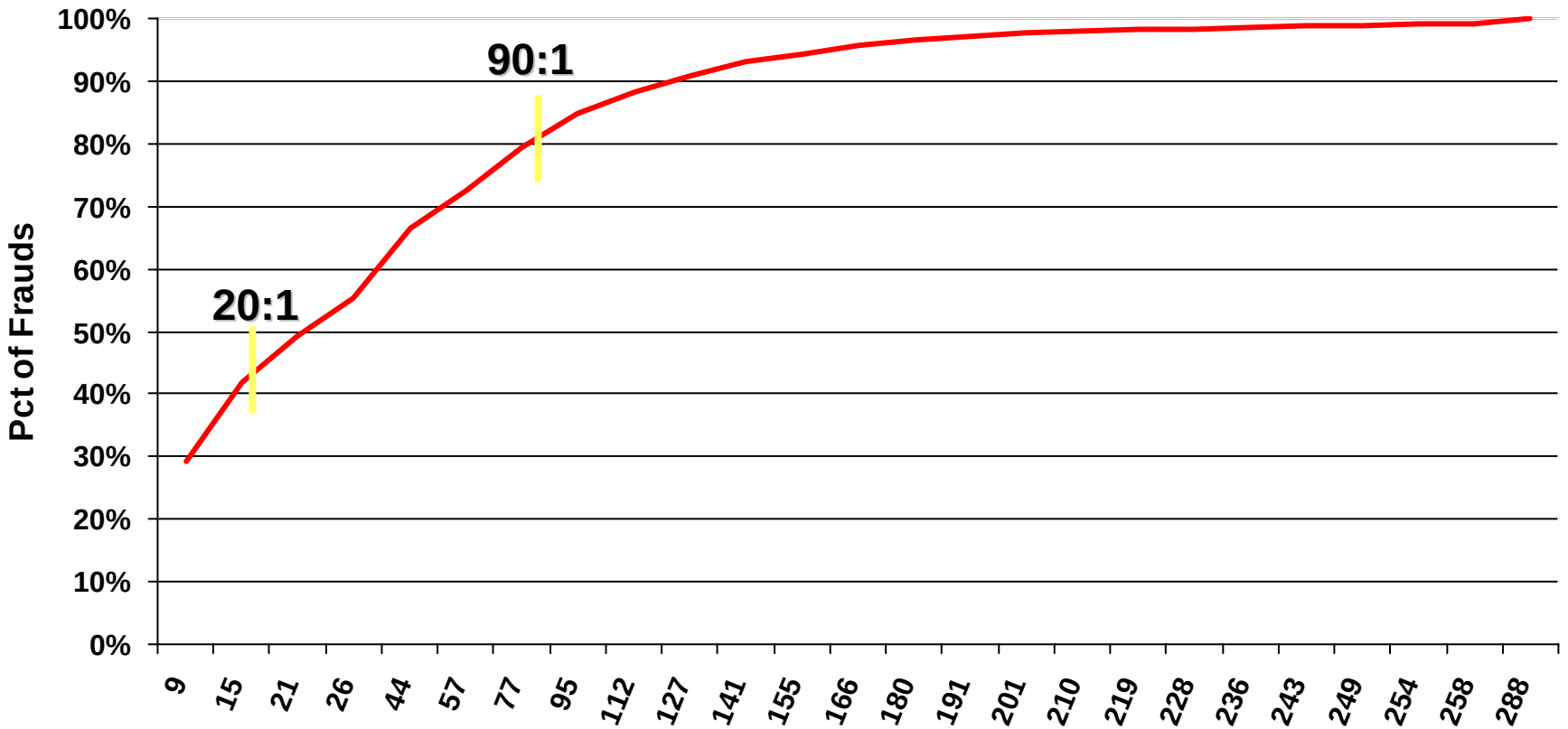
Account False Positive Rate



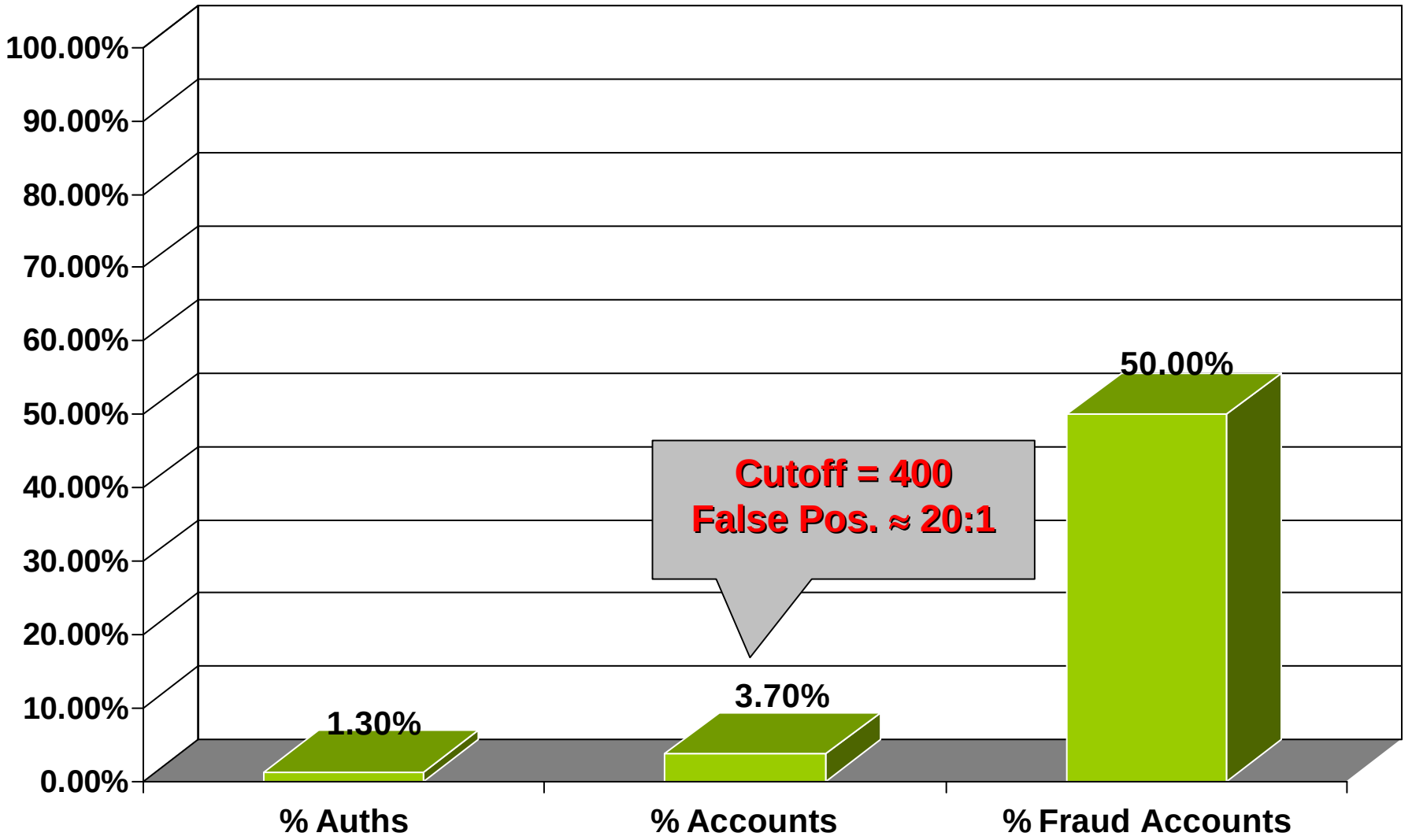
Account Fraud Detection Rate



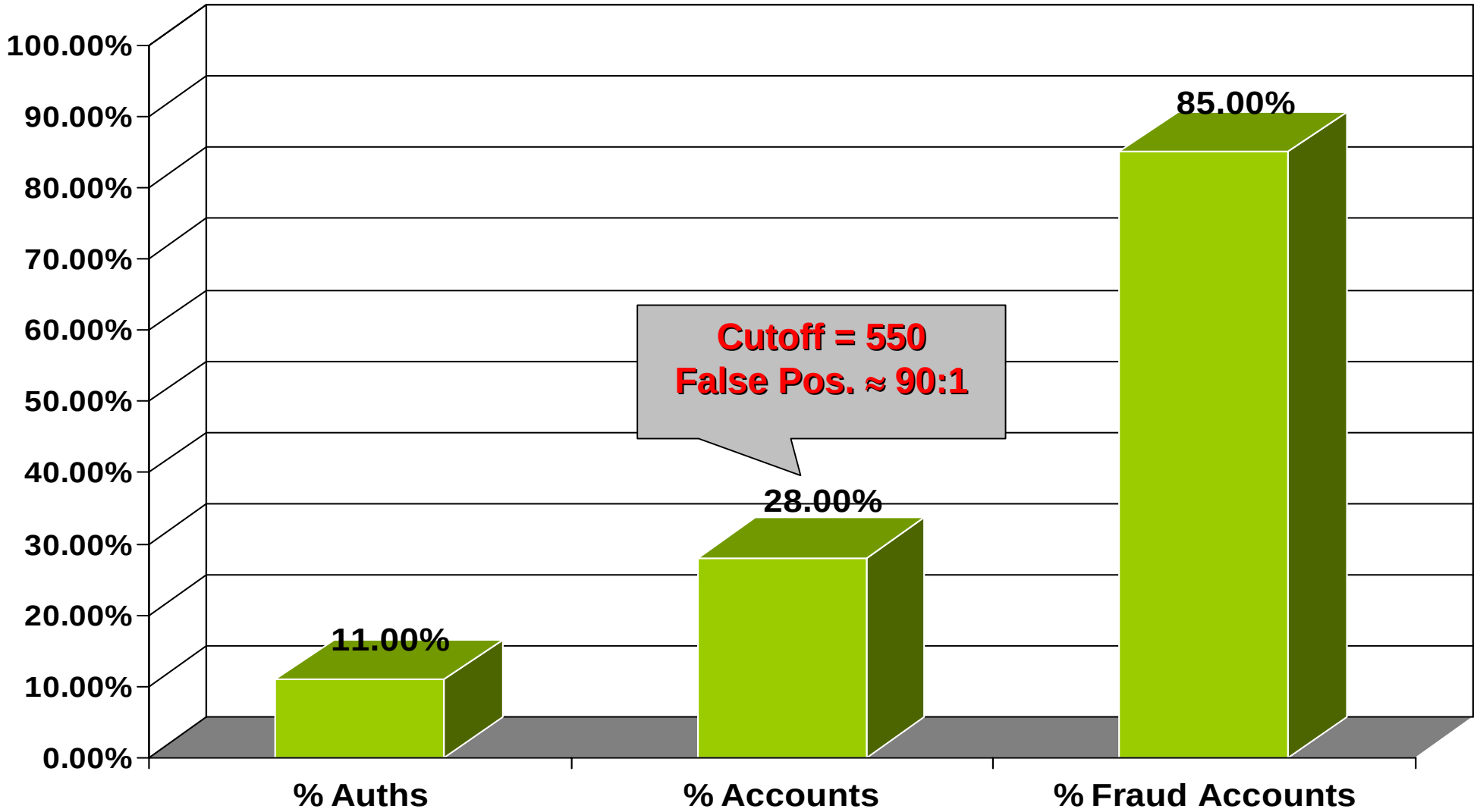
Account Fraud Detection Rate



Model performance – tradeoff



Model performance – tradeoff



Agenda

- Introduction
  - Credit card fraud losses and types of fraud
  - Authorisation and transaction flow
- Prevention and detection
  - Chip and PIN
  - Biometrics
  - Rule based system
  - Transaction fraud scoring
- Modelling process
  - Sample
  - Methodology
- Performance
  - % frauds detected
  - FPR etc.
- Score Implementation
  - Implementation mode
  - Preparation
- Monitoring
  - Performance degradation
  - Updating the model

Score Implementation

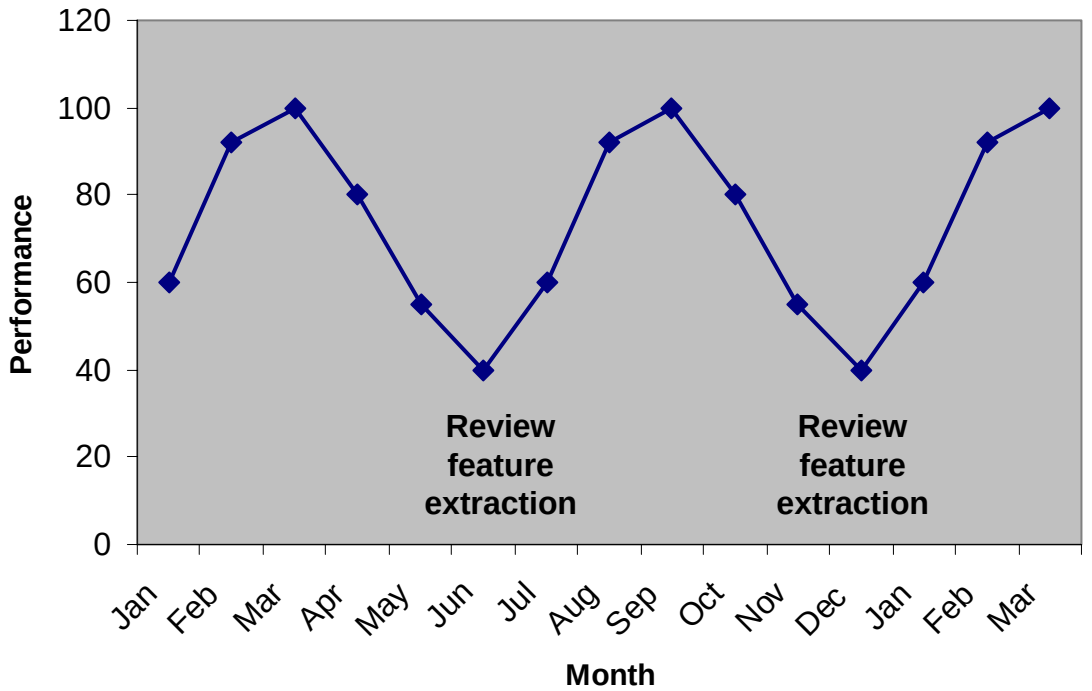
- Implementation mode
  - Batch, One behind, Real time
- Preparation
  - Verify portfolio is appropriate
  - For existing customers, build profiles prior to implementation
  - Train fraud investigators
  - Install a mechanism to facilitate regular monitoring

Agenda

- Introduction
  - Credit card fraud losses and types of fraud
  - Authorisation and transaction flow
- Prevention and detection
  - Chip and PIN
  - Biometrics
  - Rule based system
  - Transaction fraud scoring
- Modelling process
  - Sample
  - Methodology
- Performance
  - % frauds detected
  - FPR etc.
- Score Implementation
  - Implementation mode
  - Preparation
- Monitoring
  - Performance degradation
  - Updating the model

Performance monitoring

1. Biannual review of feature extraction and model fine-tune



2. Full rebuild after 18-24 months

Current developments

1. Include this technology in Secana Card Protector software

2. Apply a similar analytical approach to Merchant fraud in Secana Merchant Monitor

Transaction Fraud Scoring

John Oxley

John.Oxley@uk.experian.com

Credit Scoring and Credit Control IX, Edinburgh 2005