Intelligent Transaction Analysis for the Early Recognition of Fraud Attempts in the Credit Card business

DIMVA 2004
July 6 – 7
DORTMUND; Germany

Hanns-Michael Hepp
Intelligent Risk Management Solutions G.m..b.H.

Agenda

- Introduction
- About the "Fraud Prevention Challenge"
- 1st Generation Fraud Prevention Technology
- 2nd Generation Fraud Prevention Technology
- The Neural Net Approach
- IRIS: 3rd Generation Fraud Prevention Technology
- The Fuzzy Technology Approach
- Working with IRIS
- References and Results
- Summary

GZS Group Profile

- Biggest credit/debit card processor of Germany
- Owned by all German banks
- Key Figures (2003)
  - 920 million transactions processed
  - 7.6 million credit cards processed
  - Cross border processing for all German debit cards (~90 million)
  - More than 300'000 MC/Visa accepting merchants
  - 1'250 employees

  - IRS G.m.b.H is a 100% affiliate of GZS and a center of competence for development and marketing of intelligent risk management solutions

About the "Fraud Prevention Challenge" (I)

- Fraud losses have increased dramatically and can endanger the profitability of whole portfolios.
- 4 Billion € fraud losses in 2003 world wide (VISA and MasterCard)
- Most important segments with (card based) fraud:
  - Counterfeit/skimming
  - Lost and stolen
  - Internet fraud
  - Identity theft
  - Acquirer related fraud

About the “Fraud Prevention Challenge” (II)

- Highly skewed class distributions between genuine and fraudulent transactions. In general 99.9 % of all transactions are legal, only 0.1 are fraudulent.
- Fraud occurs in a hybrid environment and finds “weakest” point
- Fraud patterns and fraud locations change rapidly and on a global basis
- 80% of fraud amount results from authorized transactions

Fundamental Question

- How can one recognize among millions of genuine authorization requests the suspicious ones, and how can one prevent the approval of fraudulent requests without declining too many genuine transactions?

Fundamental Requirements

- Suspicious transactions must be recognized in realtime or nearly
- realtime
- Decision must be reached in realtime or nearly realtime
- False alarms must be kept at a minimum
- New fraud patterns must be recognized as quickly as possible

Characteristics of Payment transaction Data which are electronically available for building an intelligent Fraud Prevention System

- Authorization Message and SAFE Fraud Reports contain more than 30 Data Elements e.g.
  - Amount
  - Date/Time
  - Merchant Category Code
  - Country
  - POS Entry Mode
  - Merchant Name, Merchant ID
  - Terminal ID

Highly skewed Class distribution between fraudulent and legal transactions

- Generally only 1 transaction among 1000 transactions is fraudulent
- The challenge for an intelligent fraud prevention system is to predict these few transactions with a high statistical probabilty

Principal Approach to a solution

- Analysis of fraudulent data sets in comparison to legal data sets to find out whether there are significant characteristics which differ between fraudulent and legal data sets.

- This can be done by human experts using statistical tools (Expert ore knowledge based Solutions) as a heuristic process or by

- Data based solutions, where an intelligent software processes fraudulent and legal datasets and generates automatically a score which can be used for a decision .

1st Generation Fraud Prevention Technology

- "If-Then" type rules to identify potential frauds
- Alarm generation
- Dilemma “narrow" vs. “wide“

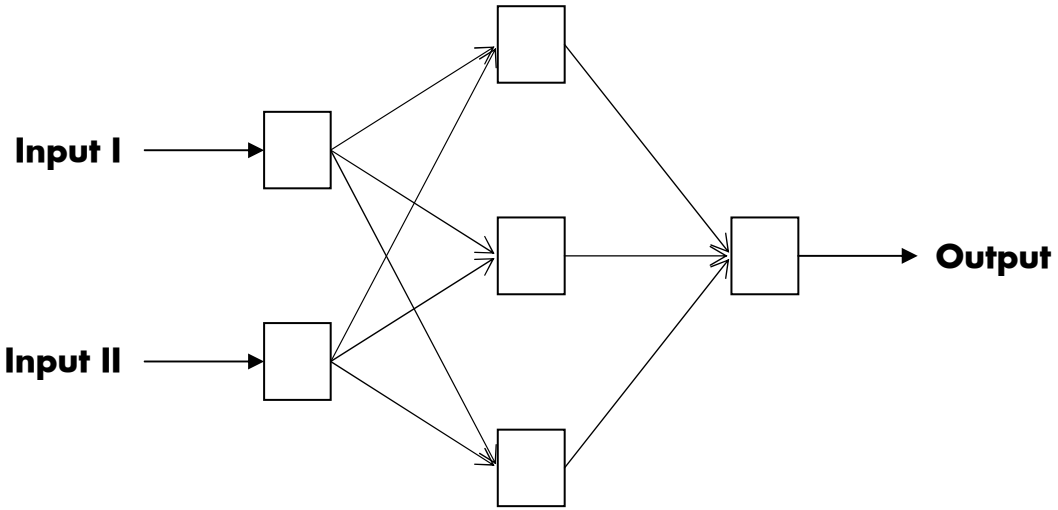
- Example: If there is an authorization request for a transaction > 1000 € from a jeweller in Miami then generate a referral. Problem: There are lots of legal transactions at jewellers in Miami, but lots of fraudulent transactions, too.

2nd Generation Fraud Prevention Technology

- Statistical and neural methods generate “typical behaviour profile“
- Transaction are compared with the individual cardholder Profile
- Risk score is built up until an alarm is generated
- Neural Net Fraud Prevention technology is widely used in the banking industry
- Example: If the neural net generates a risk score of > 950, then generate an alarm. The reason, why the neural net has calculated this score, remains unknown.

What are Neural Networks?

- Neural networks are a structure calculating a numerical output corresponding to a given numerical input.
  They are capable of adjusting themselves to the given training data in order to imitate it and to develop the capacity of generalization.



Why not use neural networks for fraud prevention?

- 10 years ago: enormous losses due to credit card fraud.
- Available historical transactional data contains detailed information of fraud characteristics.
- Neural networks are said to be able to “extract very complex mappings between features of transactions out of training data which humans cannot exploit”.
- “Neural networks learn automatically.”

The neural network experience at GZS (I)

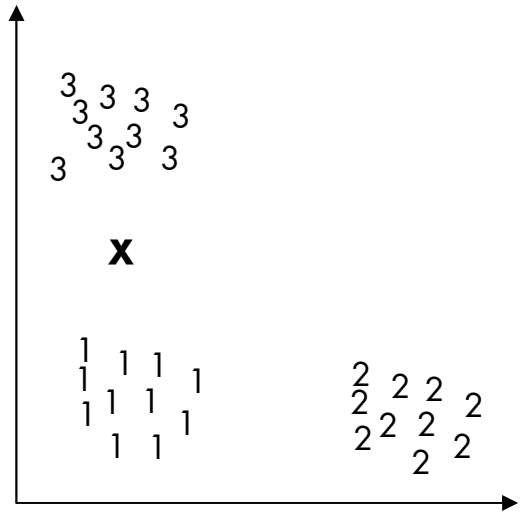
- 1995: Implementation of FALCON (HNC) at GZS
- Reduction of fraud losses followed, but the contribution of the FALCON neural net did never fully meet our (ambitious) expectations.
- FALCON contributed only 20% of the total fraud discovered by all our prevention systems.

The neural network experience at GZS (II)

- Model training of FALCON was very laborious and time consuming.
- The fraud detection rate of FALCON did not improve in four years of operation and re-training.
- We could not fit our fraud expertise with the neural net in FALCON.
- No immediate reaction on new fraud patterns was possible.
- The FALCON approach postulated a typical customer behaviour.

Reasons for the limitations of neural networks (I)

- Neural networks require analogous inputs.
- Neural networks are strongly limited in processing categorical information.



Reasons for the limitations of neural networks (II)

- Large amounts of data are needed
  - Need to fill a highly dimensional solution space
  - Very uneven class distribution
  - Difficulties to find representative training data sets
- Total dependence on past data
- Re-training is inevitable but time consuming

Reasons for the limitations of neural networks (III)

- One does not know! Neural networks are “black boxes”.
- Neural network decisions are generally not comprehensible, e.g. the reasons for a specific decision is unknown.
- Human expert knowledge about concrete fraud patterns does not help in producing better neural networks (at least with FALCON).

Intelligent Fraud Prevention – Business Demands

- Savings
- Minimum customer disruption
- Proven Return on Investment in short time

Intelligent Fraud Prevention – Technical Demands

- Meet outstanding technical standards of
  - Performance
  - Availability
- Real time recognition and reaction within the response time of the authorization request
- Easy integration into the customer's existing IT environment
- Platform independency
- Short implementation time

Intelligent Fraud Prevention – Operational Demands

- Ability to recognize and include countermeasures against new fraud patterns as quick as possible
- Consideration of local, regional, and national fraud patterns
- Integration of experts' knowledge into the system
- Ability to apply well-balanced reactions to specific fraud suspicions
- (Re-)Configuration of the decision model by business experts
- Analysis and simulation capabilities
- Ability to handle multiple portfolios

IRIS: 3rd Generation Fraud Prevention Technology (I)

- Rather than customer behaviour, fraud patterns are profiled
  - Emerging fraud patterns are detected as “infections"
  - "Fingerprints" are extracted as "DNA"
  - Detection patterns are generated as “antibodies“
- Fraud detection patterns
  - are highly selective (low false/positive rate),
  - may involve complex combinations of transactions of a card,
  - may involve combinations of transactions of one merchant or a merchant group.
- Combined technologies
  - Incorporation of first and second generation technology advantages
  - "White box“-approach
  - Efficient implementation and integration of expert knowledge with fuzzy logic

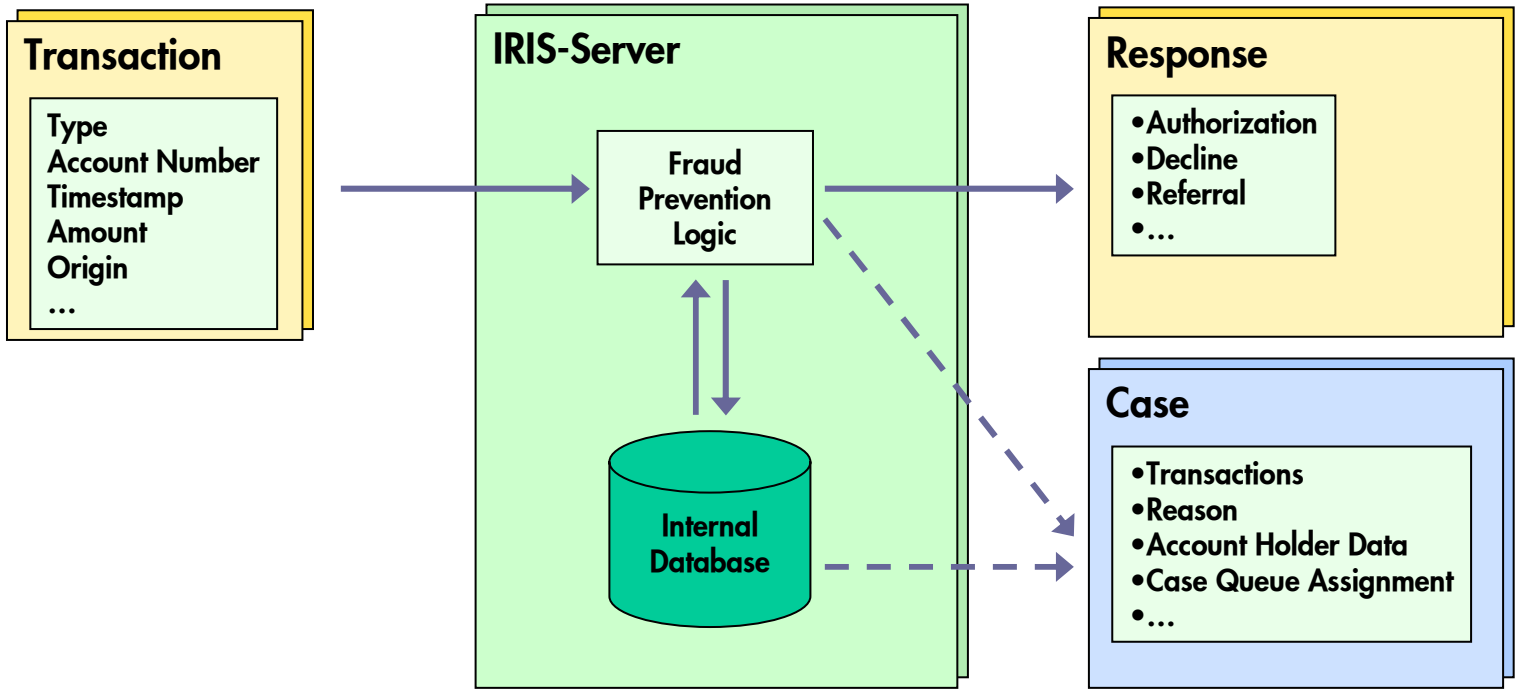
Introducing IRIS (II)

- Multi-channel solution for fraud prevention with payment systems
  - All payment systems (card, mobile, Internet, checking, withdrawal)
  - All fraud types (theft, mail loss, Internet, identity theft, counterfeit, application)
  - All parties (issuer, acquirer)
  - Multi client operation
  - Covers other areas of application like behaviour scoring, insurance claims evaluation, etc. as well
- Complete, integrated solution that meets all requirements of the process chain of security management
- Strong simulation tool to assess the potential benefit of a modification of the decision engine.

Introducing IRIS (III)

- Strongly generalized fraud prevention logic as core component
- Business Experts are always in the driver seat to integrate the latest expert knowledge into the fraud prevention logic
- Adapts powerfully to application prerequisites
  - Different transaction streams can be merged
  - Non-financial transactions can be included
  - Past transaction sequences can be evaluated
  - All input and output variables are freely configurable
  - Flexible handling of suspicion cases

How IRIS Processes a Transaction



Introducing Fuzzy Technology (I)

- Innovative technology to express human expertise
  - Business experts adopt the fraud prevention logic of IRIS
  - Knowledge can be expressed by everyday language
  - All decisions are completely transparent
- Easy to learn

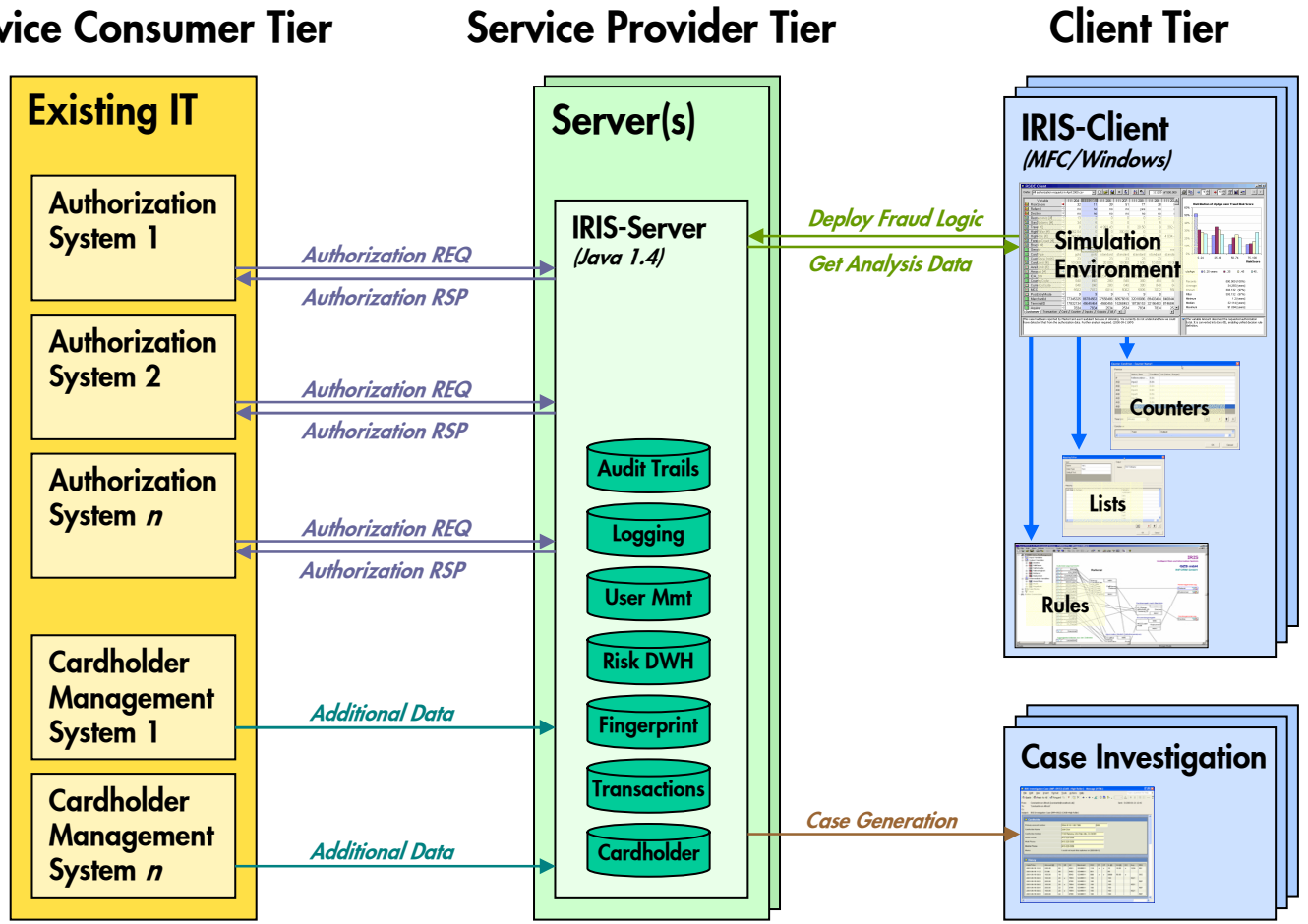
"If within *short* time *several* payments are requested from *dangerous* places and *suspicious* MCCs, fraud risk is *very high*."

Introducing Fuzzy Technology (II)

- Fast adaptation to emerging fraud patterns
  - Business experts are alerted to emerging fraud patterns
  - Countermeasures can be devised within minutes
  - No retraining or statistical recalibration required
  - No support from IT required

- Comprises other techniques
  - Neural training, statistical models, or Boolean rules can be integrated

System Structure and Integration



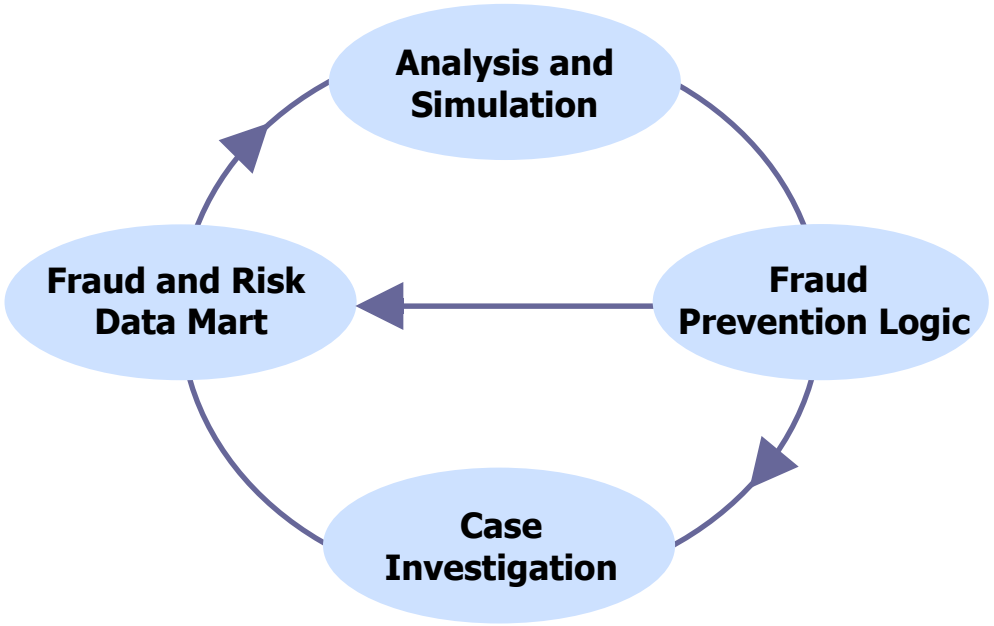
XML Interface

- Communication is based on SOAP (Simple Object Access Protocol), using XML within different protocol layers
- Transaction layer example (simplified):

```
<RSDecEng><RequestCalc>
  <Logic><Name>ATM Transactions</Name>
  <Data>
    <Var><Name>PAN</Name><Value>1234-1234-1234-1234</Value></Var>
    <Var><Name>TimeStamp</Name><Value>2003-03-27 22:10:55.412</Value></Var>
    <Var><Name>Amount</Name><Value>22.42</Value></Var>
    <Var><Name>Currency</Name><Value>USD</Value></Var>
    <Var><Name>MCC</Name><Value>4011</Value></Var>
    <Var><Name>PosEntryMode</Name><Value>keyed_in</Value></Var>
  </Data></Logic>
</RequestCalc></RSDecEng>
```

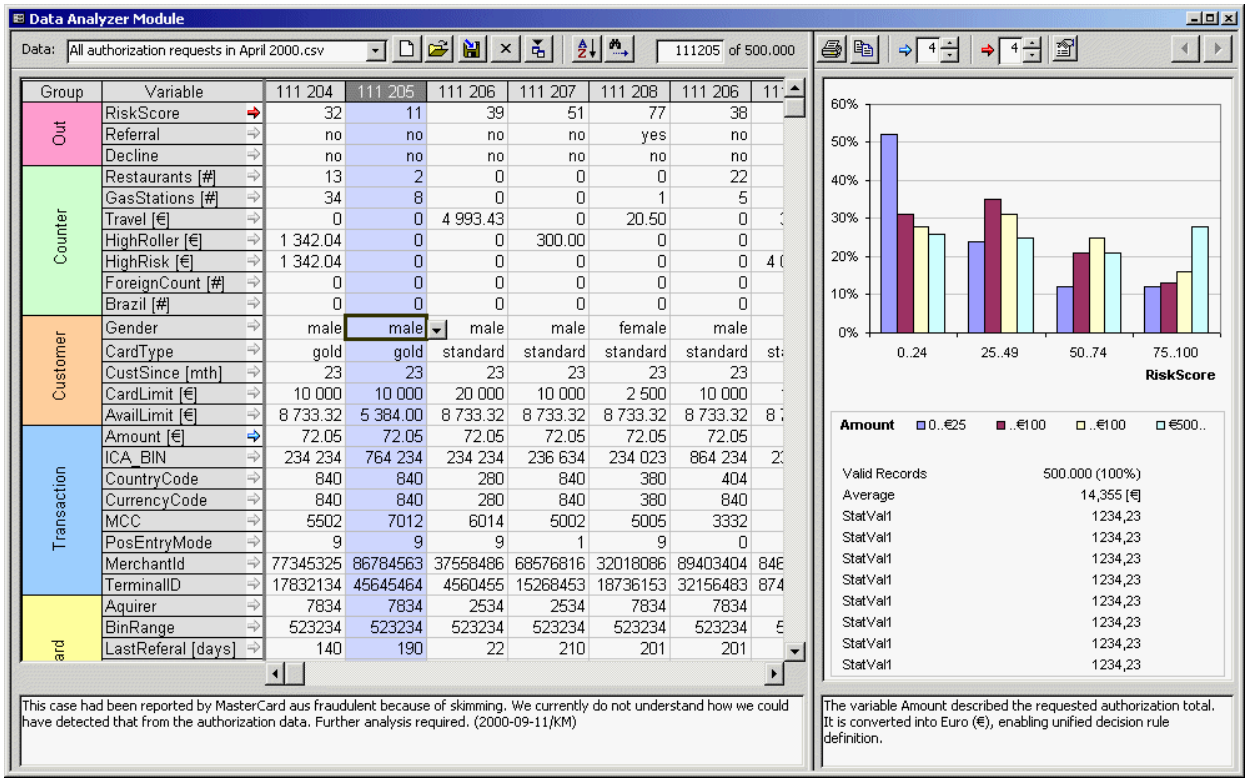
- Tolerant data linking (variables and categories)
- Burst mode for ultra-large data deliveries in tabular format
- Query layer lets service consumer ask for services and their details
- Interface can easily build from any computing environment (TAL, 390ASM, Cobol, C,…)
- Any transportation layer can be used (IP connection, http, MQ Series,..)

Working with IRIS



Working with IRIS – Analysis and Simulation

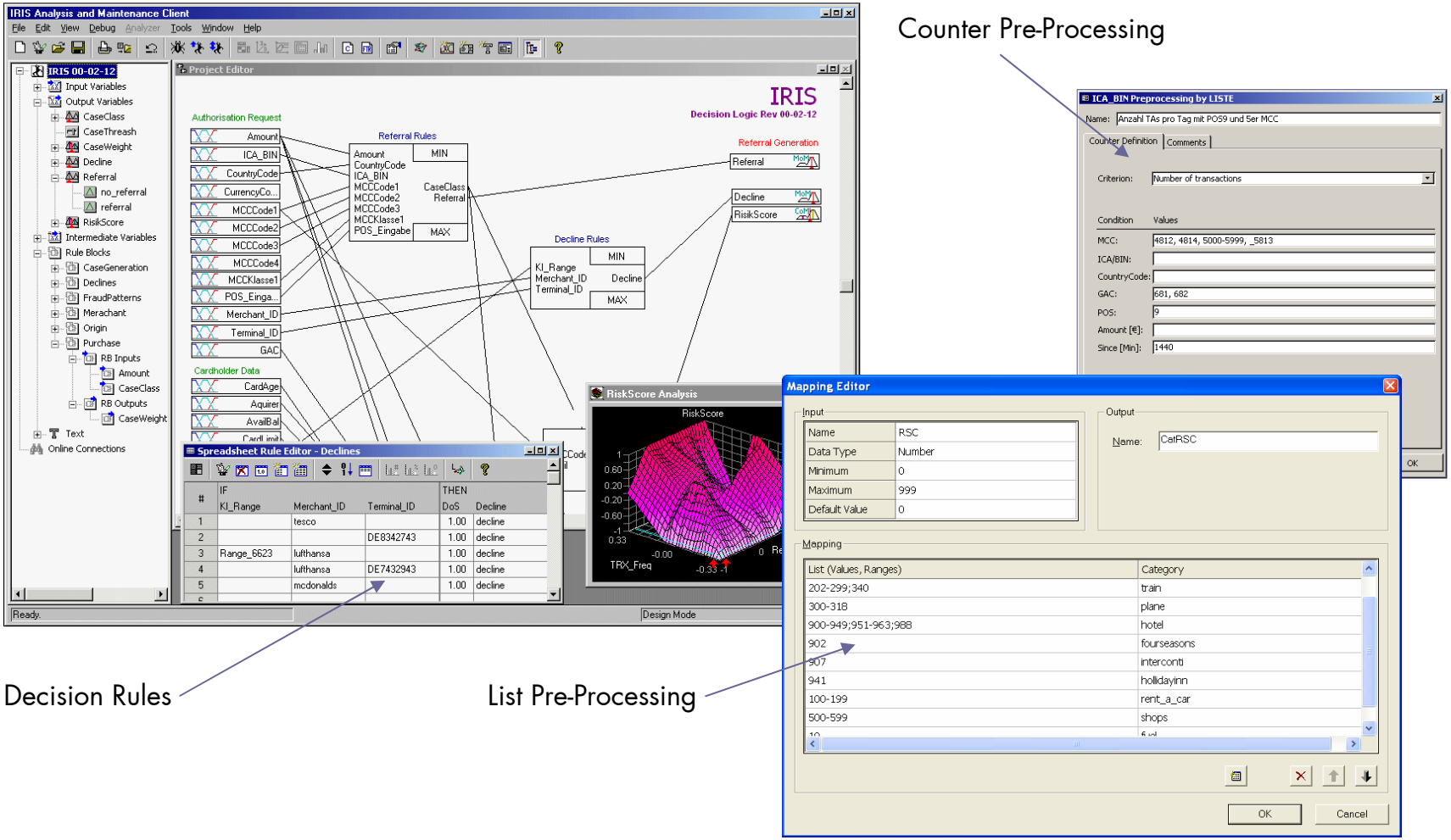
- Merging of transaction data with fraud data
- Statistical analysis
- Fraud pattern discovery
- Fraud Detection Optimization
- Continuous performance control
- Runs locally on Windows client



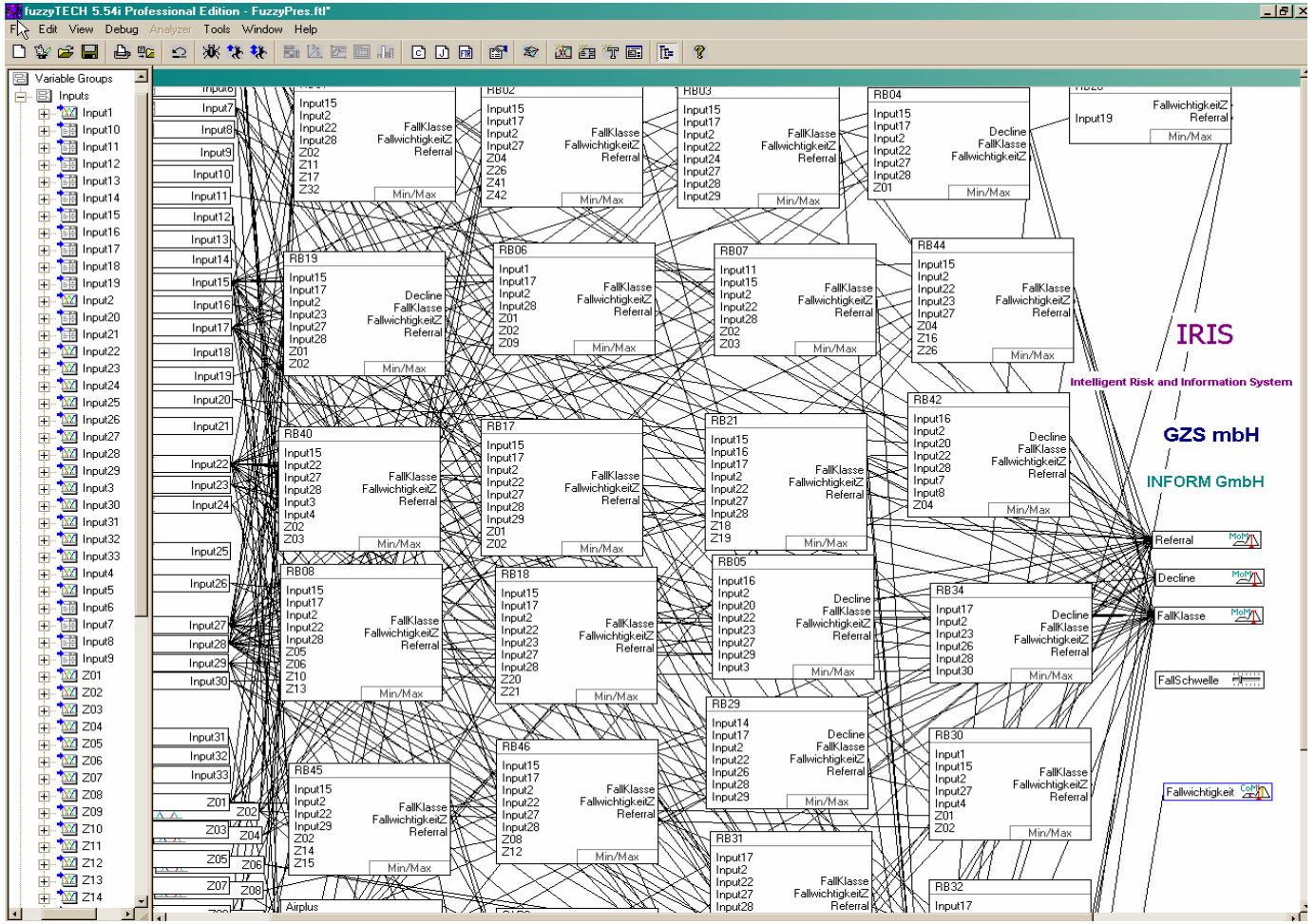
Optimization

- Optimization of Fraud Patterns within IRIS is a permanent heuristic procedure of trial and error operated by business experts and, supported by a powerful simulation tool

Working with IRIS – Decision Logic Maintenance

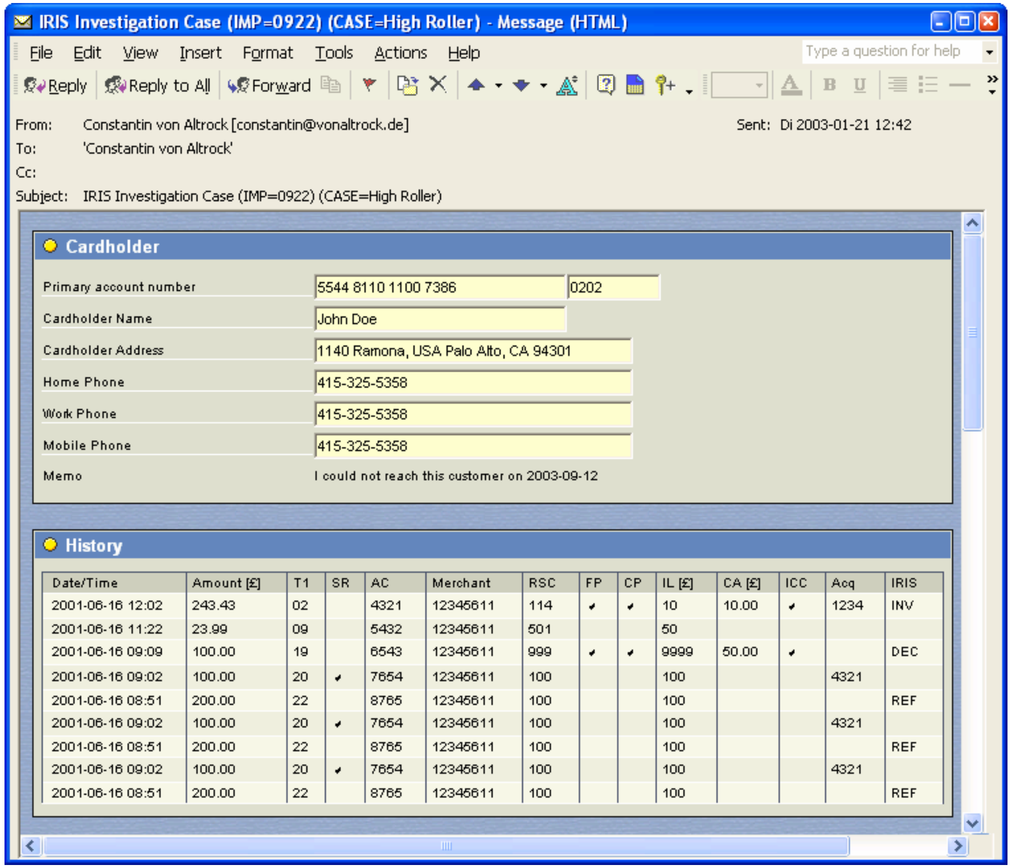


Example of a Real Fuzzy Decision Logic

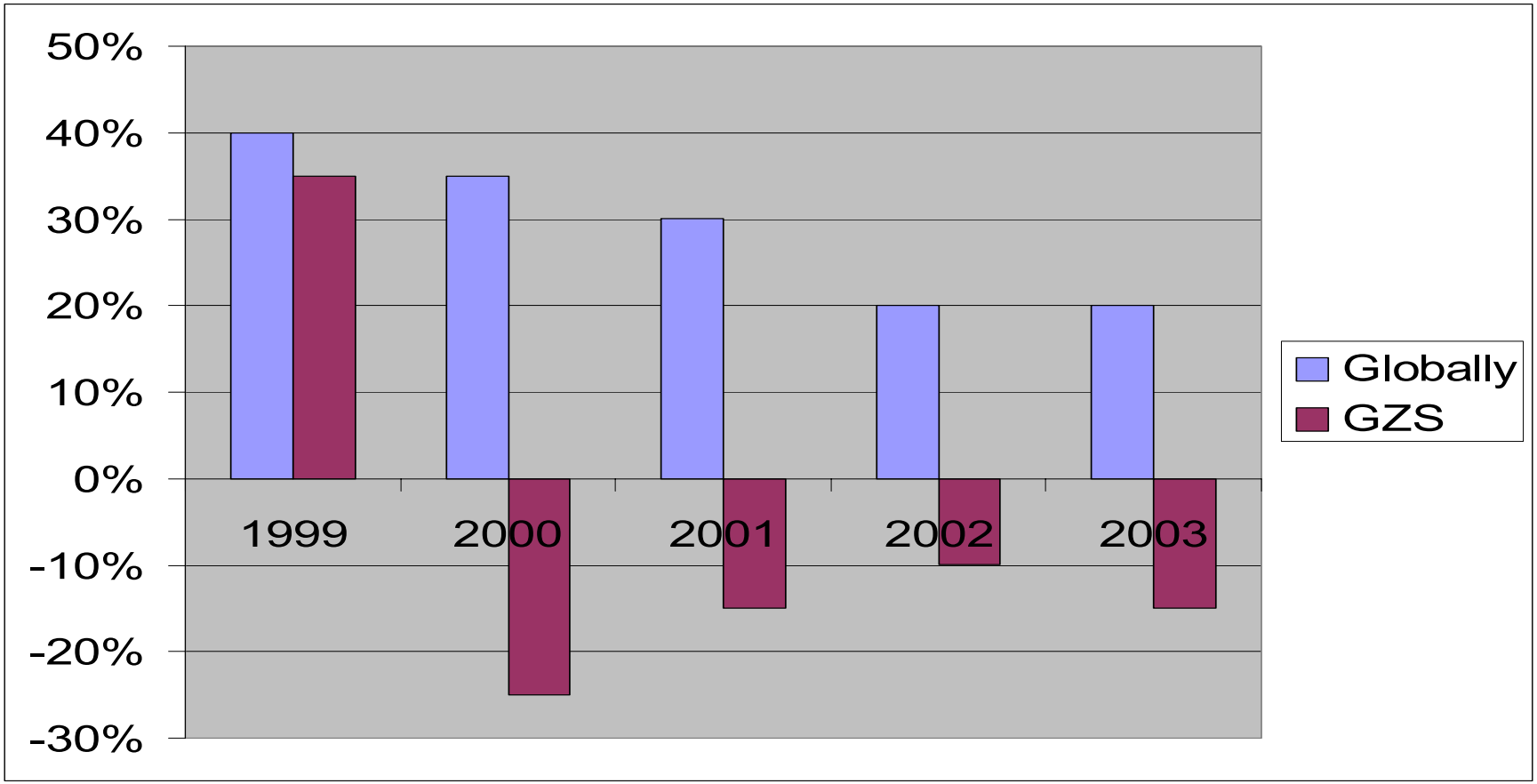


Working with IRIS – Case Investigation

- Case generation in real-time
- Decision logic can generate cases for every desired situation
- Multiple case queues can be defined
- Supports existing workflow systems, e.g.
  - Lotus Notes
  - Microsoft Exchange
  - Any email server via SMTP



Development of Fraud Losses Worldwide and GZS



Results of an IRIS Simulation

total						
legal		fraud				
number	amount	number	amount			
9.344.920	895.043.384	25.266	6.386.917			
detected (as suspicious)						
legal		fraud				
number	amount	number	amount	F/P rate	Savings	
6.145	5.004.307	2.589	1.512.538	2,37	23,68%	
13.570	10.792.862	4.188	1.972.719	3,24	30,89%	
20.559	15.208.273	5.031	2.456.885	4,09	38,47%	
39.712	21.860.941	5.785	2.821.527	6,86	44,18%	
54.554	25.565.612	6.845	3.236.756	7,97	50,68%	

Summary of IRIS Benefits (I)

- Unparalleled fraud savings, high fraud detection and low referral rate. In real life operation, the false positive rate of IRIS is about ten times better, than the neural net approach.
- Multi channel solution
- Real time operation stops fraud before it occurs
- Integrates seamlessly with existing software and hardware
- Platform independent implementation within a few months

Summary of IRIS Benefits (II)

- Rapid reaction on new fraud patterns
- Decision model optimization and rule generation by user's fraud analysts.
- Completely "white box" and transparent integration of expert knowledge
- Simulation tool allows pre-production testing

References – Life IRIS Installations (I)

- France
  - Cross-border fraud prevention for most French MasterCards
- United Kingdom
  - Switch portfolio of 7.7 million debit and ATM cards
  - VisaDebit portfolio of HBOS plc
- Switzerland
  - Viseca – 2nd biggest Swiss credit card processor (pre-life)
  - Acquirer fraud prevention (pre-life)

References – Life IRIS Installations (II)

- Germany
  - MC/Visa portfolios of >2'000 banks including Deutsche Bank, Commerzbank, and DZ Bank
  - Acquirer fraud prevention for 330'000 merchants
  - 45 million debit and ATM cards (EC, Maestro) international fraud prevention
  - Mobile payment fraud prevention for 27 million GSM phones

References – IRIS Technology Users

Business Case

- IRIS implementation saves 30-40% of card fraud
- ROI within 0,5 - 2 Years

Summary

- IRIS is a successful example of a European technoloy development against heavy competion in advanced markets

- Though we have sponsored 6 research projects at RWTH Aachen and University of Frankfurt, to train neural nets with credit card data we never had a result that could match the performance of expert knowledge driven solutions. We are continuing our training efforts with neural nets but until today we did not achieve better results

- Nevertheless more than 60 % of the big credit card issuers in the US and U.K. still use the Neural Net Approach