Sources Cited


https://github.com/cazala/synaptic/wiki/Architect


http://www.statisticbrain.com/credit-card-fraud-statistics/
Overview

- Introduction to card fraud with statistics
- Properties of an AI system that helps with fraud prevention
- Theoretical look at Neural and Bayesian Networks
- Some examples of fraud systems cost-benefit analysis
Types of Card Fraud

1. Bankruptcy fraud: in which a cardholder makes charges to their card with the intention of declaring bankruptcy and no intention of ever repaying balances

2. Application fraud: in which an application is submitted with false information (e.g. inflated income) or fraudulent information (e.g. stolen SSNs)

3. Behavioral fraud: in which an online transaction is completed by using any credit card unbeknownst to the cardholder

4. Theft/Counterfeit fraud: in which somebody presents a stolen credit card and pretends to be that person in order to make a transaction

Credit card fraud statistics

Percentage of Americans who have been victims of credit card fraud: 10%

Median amount of reported credit card fraud: $399

Percentage of all financial fraud due to credit card fraud: 40%

Total credit card fraud worldwide: $5,550,000,000 ($5.5 billion)

Using counterfeit cards: 37%

Using lost or Stolen cards: 23%

http://www.statisticbrain.com/credit-card-fraud-statistics/
How AI can prevent financial fraud

Using big data to determine what should be classified as normal activity

Using up-to-date information to determine if a customer(s)’s actions can be constituted as regular or irregular activity

The system must be able to adapt to both changes made by normal customers’ actions, and the fraudsters’ evasion tactics
Necessary Properties of Fraud Detection Systems

Able to choose training sets to minimize skewed data

Able to clean data to handle noise or missing information

Should be aware of possibility of overlapping data, in which fraudulent charges appear genuine and genuine charges appear fraudulent

Able to adapt to new, sophisticated methods of fraud that evolve over time

Able to generate useful metrics about itself

Considers the cost of the fraud and the cost in resolving it
Credit Card Fraud Detection with Artificial Neural Networks

Can be implemented with Feed Forward Multi-layer Perceptron

This requires three layers in the network: an input layer, a hidden layer, and an output layer

https://github.com/cazala/synaptic/wiki/Architect
Credit Card Fraud Detection with Artificial Neural Networks

The neural network learns by Backpropagation of Error Signals, which includes two passes:

A forward pass provides a node or perceptron a summing and activation function to generate its output.

A backward pass calculates an error at the output layer, then propagates backwards to attach corrections to inner layers’ outputs.
Credit Card Fraud Detection with Bayesian Networks

Must identify topology of directed acyclic graph using STAGE, an instance of global optimization

Generate training data by continuously optimizing objective and value functions

Neural vs. Bayesian Networks Results

<table>
<thead>
<tr>
<th>experiment</th>
<th>±10% false pos</th>
<th>±15% false pos</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANN-fig 2(a)</td>
<td>60% true pos</td>
<td>70% true pos</td>
</tr>
<tr>
<td>ANN-fig 2(a)</td>
<td>47% true pos</td>
<td>58% true pos</td>
</tr>
<tr>
<td>ANN-fig 2(c)</td>
<td>60% true pos</td>
<td>70% true pos</td>
</tr>
<tr>
<td>BBN-fig 2(e)</td>
<td>68% true pos</td>
<td>74% true pos</td>
</tr>
<tr>
<td>BBN-fig 2(g)</td>
<td>68% true pos</td>
<td>74% true pos</td>
</tr>
</tbody>
</table>

The Bayesian network was more accurate and had faster learning times

The neural network evaluates new examples faster

Determining the best configuration of weights of a neural network using Simulated Annealing

Using the data

The data in this paper was broken down into two separate sets.

The simulated annealing was run on 75% of the data for the purposes of training and setting the weights of the neural network.

The other 25% was used to evaluate the network using the weights that were set by the aforementioned 75% of the data.

The training phase took nearly two days to get the weights set correctly, which resulted in a 1% error in classifying the training data as fraud or non-fraudulent.

Running the weights on the 25% of the data used for evaluation

Conclusions from Real-Time Credit-Card Fraud Detection using Artificial Neural Network Tuned by Simulated Annealing Algorithm'

The simulated annealing had a somewhat long (2 days to learn from 750 test cases) learning period but had a considerably high

It correctly identified 92% of fraudulent cases

It correctly identified 85% of non-fraudulent cases

Two Approaches to Fraud

There are two main ways industry can deal with fraud:

Deal with fraud after the fact

- Requires no prevention infrastructure
- Never inconveniences customers with untimely declined authorizations
- Expensive to absorb or try to reclaim losses
- Collaboration with outside agencies necessary (i.e. law enforcement)

Deal with fraud before it occurs

- Requires a great deal of infrastructure (timely and costly)
For SPNB, trying to resolve fraud after the fact was determined more expensive than preventing fraud.

In 1987, SPNB commissions a Fraud Task Force to develop an expert system through its corporate security department.

Expert system implemented bank-specific and industry-wide rules for weighing the likelihood of and detecting fraud.

After going live in 1988, system paid for itself in two months.
American Express’ “Authorizer’s Assistant”

In 1988, AMEX transitioned from human-only card authorizations to human/automated blend. Prior to transition, authorizers would glean information from computer screens and choose whether or not to approve each individual transaction. American Express had to balance the following concerns:

Human authorizations are expensive and take too long

System ideally needed to be in place at all times of day to approve transactions

Human authorizations would eventually be overwhelmed by the number of transactions needing approvals

Too many card declines and customers would be unhappy

Too liberal with approvals and AMEX would have to absorb the fraud losses
Authorizer’s Assistant (AA) Timeline

July 1985: American Express issues competitive RFP.

October 1985: Contract between American Express and Inference is signed.


March-April 1987: Acceptance testing by American Express; AA Pilot in experimental on-line use at one operating center.

May-August 1987: Deployment ROI analysis; AA Rollout design phase.

September 1987: American Express decision to deploy AA.


May-July 1988: Integration testing.
Authorize’s Assistant (AA) Features

Authorize’s Assistant would gather the same information that a human authorizer would use. Where possible, AA would approve transactions.

If something landed in a “grey zone” it was referred to a human.

AA provided human authorizers with a number of better aggregated and organized screens so that human authorizers had better information with which to decide transaction approvals.

AA was validated using a heuristic approach, getting run on thousands of transactions and guided by human authorizers.
Authorizer’s Assistant (AA) Impact

Half as many cases ended up getting referred for collections and fraud

Authorizations being declined decreased by 33%

AA as an assistant improved human authorization productivity by 20%, and on that alone would pay for itself in less than two years

Savings on decreased collections and fraud referrals were more than five times the savings the system had on increased human productivity
Conclusion Looking at Real Life Examples

AI systems can take time and money to implement.

They require a multidisciplinary approach and often necessitate commissioning of outside experts and companies.

Once rolled out, however, AI systems pay for themselves by doing things more quickly, with more reliability and stability, and more scalability.

Updates may be necessary as business requirements change, new policies are adopted, regulations are implemented, or customer/fraudster patterns change, but these updates are easier once a system is already in place.