



Case Study

Implementation of Samport ZEUS in a High-Risk Company



1. Summary

In July 2006 a company in the prepaid gift card industry went live, selling virtual gift cards to customers world wide. From October till December 2006 they suffered high rates of chargebacks due to card-not-present fraud and the trend was increasing. Around Christmas the Company signed a contract with Samport including fraud management and card processing. Samport identified some key problems and the Company introduced automatic risk rules accordingly. The fraudulent transactions dropped quickly during spring 2007. In March, the Company employed the Samport ZEUS fraud screening software. The company's chargebacks dropped further to a steady level of 0.2 – 0.3 per cent.

2. The Company

The company started business in July 2006. Turnover was very limited and can best be described as live testing. No advertising was made until August-September. The main product was a virtual gift card. The customer buys cards at fixed rates. Most customers buy cards worth 5-10 USD. The Company also has several business clients that have an auto recharge deal, meaning that as soon as the virtual prepaid card is used up another is automatically purchased without active intervention from the customer (recurrent billing).

The Company's business rules:

- Only two payment cards per account
- Max limit of \$12 per month the first month
- Max limit of \$120 the following months.
- No transfer of payment card between active accounts

However, no velocity rules were employed. In fact the Company did not have any professional anti fraud system installed at all as the company had little fraud awareness. Transactions from all countries were allowed, as were all payment cards.

3. November 2007 - First Fraud Wave

In late November the Company noticed an increase in fraudulent attempt. The denied transactions (bank denial) increased as did the amount of chargebacks. The typical pattern was that a user would create multiple accounts and try different credit cards. They also changed the credit card for the same account (cancelling the old one and registering a new card). In October the transaction volume peaked at 5,500 transactions.

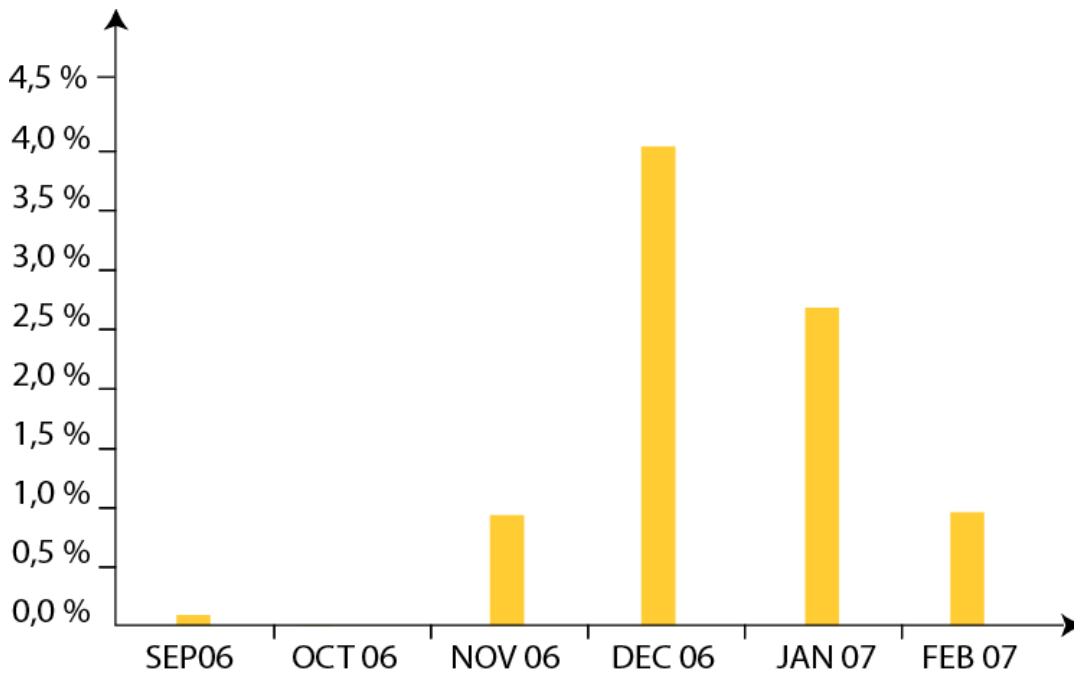
At this point the company was only partly aware of the fraud threat and did not fully understand the consequences and appropriate counter measures. The acquiring bank contacted the company and issued a strong warning. The Company tried to refund several of the suspected fraudulent transactions, thus neutralising a would-be chargeback.

Samport and the Company signed a contract in December 2007. Samport immediately advised that some countries should be blocked. A list of "negative



countries” was created and implemented. Together with manual screening the amount of chargebacks dropped quickly.

A graph of the confirmed chargebacks for the period:



Graph 1: The absolute amount of chargebacks in percentage as reported by the acquiring bank per month. Surveys reveal that there is an approximately 80 days lag between the fraud and the reported chargeback.

As stated above, the Company refunded many of the transactions made in Nov-December, suspecting that they were fraudulent. The risk manager at the time surmised that they would probably have suffered 10-15 per cent chargebacks, had not the refund been done.

4. Samport ZEUS

In March 2007 the Company started utilising Samport ZEUS 1.2 anti fraud software. The installation went as scheduled without any major show stoppers. The response time for each transaction during peak time was 0.4 seconds. Samport ZEUS returns codes corresponding to the authorisation outcome and the fraud check:

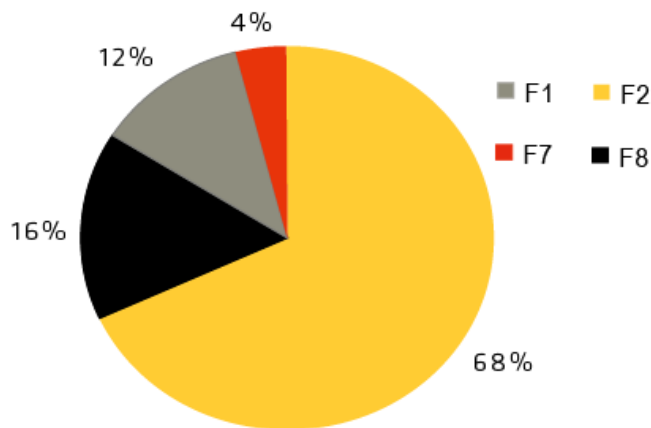
00	approved
01-99	not authorised
F1-F8	fraudulent transaction



Key:

- F1 = Artificial Intelligence (pattern)
- F2 = Artificial Intelligence (entry pattern)
- F5 = BIN – IP country mismatch
- F6 = Negative Country
- F7 = Geo Tech (geo pattern triangulation, MAC codes etc)
- F8 = Velocity

The outcome of the “F” response codes for the Company was as follows (sample June 2007):

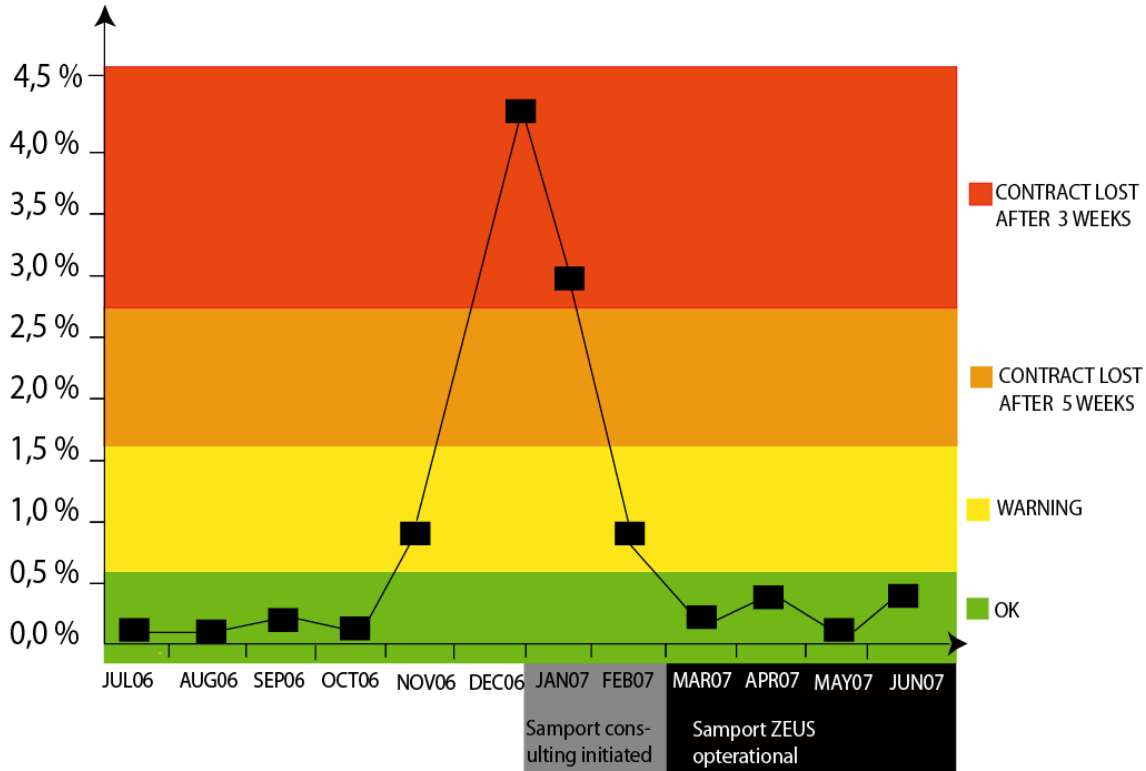


Graph 2: The high amount of F2 codes returned by Samport ZEUS implies active fraudulent attempts. Samport ZEUS analyses the input pattern at the time of order placement and produces the F2 code if the pattern corresponds with known fraudulent behaviour. There is a strong correlation between the “F2 behaviour” and known fraudulent cases. The F8 code (velocity) is also a very strong indicator of fraud, i.e. repetitive transactions from the same IP address and/or card usage.

Samport’s Risk department also carried out forensic analysis on the pre-Samport ZEUS chargeback cases and found that the fraudulent behaviour was consistent with the Samport ZEUS programming.



Chargeback statistics of the period June 2006- June 2007:



Graph 3: The monthly chargebacks as reported by the acquiring bank. The statistics is in absolute numbers of chargebacks divided on total transactions. Note that the “warning” section (yellow) is actually stricter – 0.5 per cent - depending on card scheme (VISA/MC)

The conclusion is that Samport ZEUS anti fraud system significantly contributed to bringing down the chargeback rate from February’s 1.1 per cent to 0.2 per cent. However, it should be noted that the fraud rules implemented in Dec – February also contributed greatly to keeping fraud in check.

The immediate benefit for the Company was that they could divert staff from manual vetting as Samport ZEUS operated 24/7 with an automated yes/no decision. The company did, however, choose to set Samport ZEUS to warn only, preferring to reject the suspicious orders manually. In May they were confident enough to set Samport ZEUS to automated rejection. In almost all cases the Company did reject an order when warned, so the actual difference was inconsequential.

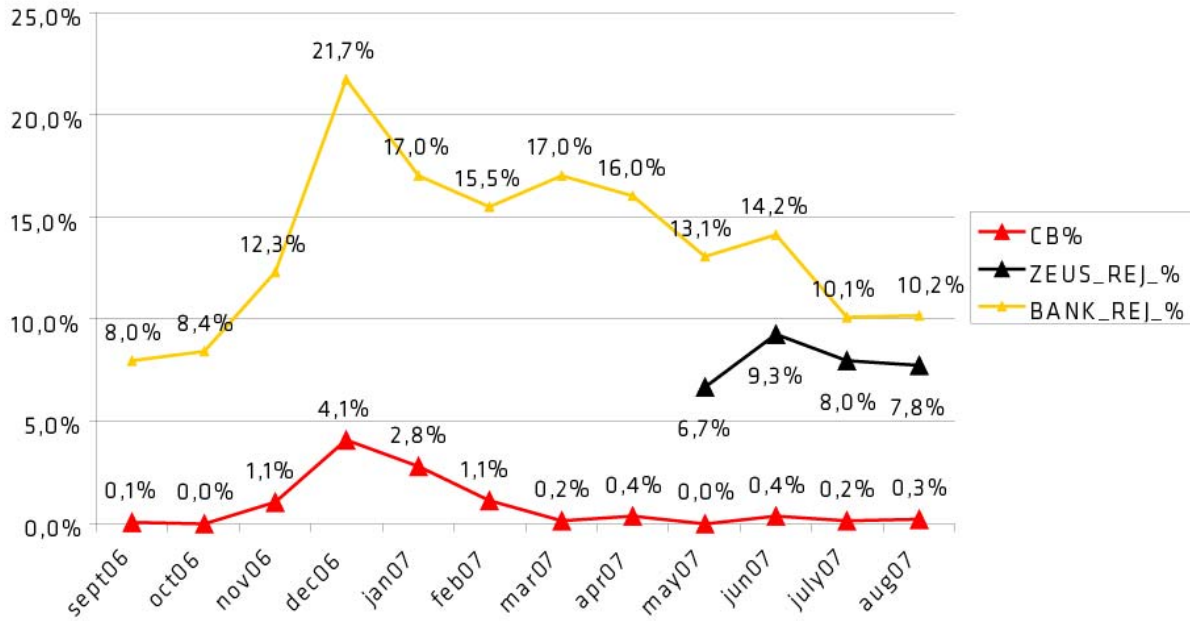
5. The Effect on Sales and Conclusions

For an end user it is equally important to balance the reduction in fraud with the overall rejection rate. The ideal situation is a low rate of rejected orders with a low rate of chargebacks. However, as fraud is dynamic, a sudden peak in rejected orders is not bad; it simply suggests that there is an increase in fraudulent activity and that



the fraud prevention system actually works. In a medium – long term perspective a solid system should have a low and steady rejection rate.

Data for the first period:



Graph 4: the combined data for the Company’s rejections rate split by not authorised and Samport ZEUS. Not that ZEUS was set to “Warn” during March-April, hence the missing data. The bottom line (red) indicates chargebacks.

Analysis: Samport ZEUS rejected between 7-9 per cent of all transactions during the summer of 2007. It is a fairly high rate and is best explained with that the Company is operating in a very exposed industry. The most important fact is that the non-authorised transactions dropped significantly when Samport ZEUS was switched on. The conclusion is that Samport ZEUS rejects transactions that would not be authorised by the bank, as most fraudulent attempts. In effect, Samport ZEUS keeps the chargeback rate below the critical 0.5 per cent while rejecting 7-9 per cent of the orders. A large part of these rejected orders would not be authorised anyway so the overall impact on sales is small.

One year later after the fraudulent attacks November 2007- January 2008 the Company’s transactions has increased significantly. They now have approximately 40,000 transactions per months and Samport ZEUS rejects approximately 6 per cent of all transactions. The acquiring bank reports very few chargebacks (data for 2007 still pending).

About Samport

Samport specialises in helping banks, large merchants and system vendors make sure they can handle the demands on secure, effective and cost efficient transactions, whether through payment over the Internet or in retail stores. We make this possible through our two market leading products; Samport LETO and Samport ZEUS.