



## Viseca Card Services reduces fraud loss with SAS®

Advanced analytics improve the bottom line by reducing fraud losses by 15 percent

### Industry

Retail Banks

### Business Issue

Prevent losses by detecting and preventing fraud on Viseca Card Services' 1 million credit cards and more than 100,000 daily transactions.

### Solution

SAS® Enterprise Miner™, SAS® Enterprise Guide®, SAS Text Miner and SAS BI Server.

### Benefits

Eighty-one percent of all fraud cases are found within a day, and total fraud loss has been reduced by 15 percent. Even as the number of fraud cases across the industry has doubled, Viseca Card Services has reduced loss per fraud case by 40 percent.

Explosive growth in online shopping has sparked a flood of credit card fraud. Switzerland's largest credit card company, with 1 million cards, now uses advanced SAS Analytics to stop the cheating and improve its bottom line. Viseca Card Services has reduced losses due to fraud by 15 percent – a record few credit card companies can match.

Credit card crooks face tough odds when they try to swindle with a card issued by Viseca Card Services. The Swiss credit card giant uses advanced SAS Analytics and data mining in its battle against fraud, and the results are impressive and measurable. Even though the fraud cases throughout the industry have doubled in the last two years, Viseca Card Services has reduced loss per fraud case by 40 percent. These are results that go straight to the bottom line. As Viseca Card Services Business Analyst Marcel Bieler says, "Every dollar not fraudulently spent is a dollar earned."

"Credit card profit margins are approximately a tenth of a percent, so it makes excellent business sense to focus on early fraud detection," says Bieler.

"Credit card companies can save significant money by applying advanced business analytics to minimize fraud."

According to Bieler, Viseca Card Services has an online system in place capable of catching about 60 percent of all fraud cases immediately. With the aid of offline analysis using SAS, Viseca Card Services now catches more than

80 percent of all fraud cases within 24 hours.

"Thanks to SAS Analytics, our total fraud loss has been reduced by 15 percent," says Bieler. "We have one of the best fraud prevention ratings in Switzerland, and our business case for fraud prevention is straightforward: Our returns are simply more than our investment."

### Profits at peril

With 1 million credit cards and more than 100,000 daily transactions, Viseca Card Services is the largest credit card issuer in Switzerland. The company uses SAS to optimize the effects of its marketing campaigns, building its market share to 25 percent. While profits are healthy, they are affected by losses incurred due to increased credit card fraud. That is why the company's central analysis team was given the critical task of providing the insight necessary for fact-based decisions by the Fraud & Risk Department. It is here that staff can react immediately to even the smallest sign of credit card fraud.

### Real-time card authorization

Viseca Card Services uses SAS for offline fraud analysis. An external decision engine drives the authorization process that begins when a card is used in a shop. If there is any sign of cheating, the system sends an automatic alert to fraud agents at Viseca Card Services, who then telephone the card owner before the transaction is either completed or denied. The extensive control process takes place within seconds and is carried out for

“Thanks to SAS Analytics our total fraud loss has been reduced by 15 percent.

We have one of the best fraud prevention ratings in Switzerland and our business case for fraud prevention is straightforward: Our returns are simply more than our investment.”

- Marcel Bieler, Business Analyst, Viseca Card Services

every one of the more than 100,000 daily transactions handled by the company. The rules guarding that decision engine are based on the analysis of past fraud cases. The use of SAS for this analysis is key to Viseca's success.

### **Battling phishing and pharming**

When a card is used online, offline analysis begins immediately. Because the Internet is where credit card fraud is growing most rapidly, it is here that Viseca Card Services has ramped up its analytical detective work the most. Among other types of fraud on the rise are phishing, in which fake e-mails are sent in the name of card issuers like Viseca Card Services, and pharming, in which fraudulent Web sites attempt to trick users into typing in their credit card information.

“We've had a lot of success using SAS to prevent cheating and to minimize losses if a breach does occur,” says Bieler. “Pattern recognition and case-based analyses help us prevent a lot

of fraud before it happens. Within the last two years, we have also used data mining to minimize fraud transfer after a fraud has occurred. The SAS analytical framework has really proven its worth here and has reduced loss per fraud case by 40 percent.”

Bieler's comment referred to Project FRAUDO (Fraud Risk Analysis Using Data Offline), which Viseca Card Services initiated as its latest weapon to defeat Internet fraud by rapidly connecting credit cards to fraudulent transactions.

### **Needle in a haystack**

The company's customers perform between 20,000 and 40,000 online transactions per day – and all are checked for fraud. FRAUDO and data mining enable Viseca Card Services to find the transactions that look suspicious and concentrate efforts on them.

“Ninety-five percent of the time, there is nothing wrong. But the last 5 percent – it's bingo,” explains Bieler. “Five percent

may not sound like much, but it adds up to a few cases every day. Fraud losses are so high that it makes it worth checking the other 95 percent where there may be nothing wrong. The investment payback begins at 3 percent. We cannot stop people from cheating, but we can minimize the financial consequences. There is no better partner than SAS for this job.”



**SAS Institute Inc. World Headquarters +1 919 677 8000**

To contact your local SAS office, please visit: [www.sas.com/offices](http://www.sas.com/offices)

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. 104537\_S43806.0510

The results illustrated in this article are specific to the particular situations, business models, data input, and computing environments described herein. Each SAS customer's experience is unique based on business and technical variables and all statements must be considered non-typical. Actual savings, results, and performance characteristics will vary depending on individual customer configurations and conditions. SAS does not guarantee or represent that every customer will achieve similar results. The only warranties for SAS products and services are those that are set forth in the express warranty statements in the written agreement for such products and services. Nothing herein should be construed as constituting an additional warranty. Customers have shared their successes with SAS as part of an agreed-upon contractual exchange or project success summarization following a successful implementation of SAS software.