

Samport ZEUS - Anti Fraud System



The SAMPOR ZEUS - Anti Fraud System is a software that detects and stops fraudulent payment card transactions online. The product can be used by e-commerce merchants or acquiring banks. SAMPOR ZEUS can either be hosted or integrated in the customers' IT infrastructure, and stops fraudulent transactions before authorisation takes place. Once operational, SAMPOR ZEUS works 24/7 without any need for human intervention.

1. Concept

A fraud prevention system is loosely derived from a traditional credit report – a cornerstone in assessing whether to offer a loan to a client or not. The credit report weighs up historical data and produces a credit limit that can be offered to the applicant with a reasonable risk. The bottom line is that the less income a client has had and the more default payments, the worse credit scoring he or she will get.

When vetting a customer shopping on the Internet, these methods are not applicable. The data available is limited to customer name, address, payment card details and the type of commodity purchased. Initially, the creators of AFS relied heavily on lists of “hot” payment card numbers and addresses. Once a payment card had been used in a fraudulent transaction, it was listed together with the name and address of the perpetrator. However, this is not practical, for a variety of reasons. The next method involved collecting the order data of fraudulent transactions. Through this method it was possible to see that fraudulent orders distinguished themselves from genuine orders. Typically, the fraudulent orders contained free email accounts, were placed late at night or contained many of the same type of products, quite the opposite to a normal consumer’s needs. Once enough data has been accumulated it becomes relatively easy to separate genuine orders and compare them with fraudulent orders.

The AFSs evolved into a predicting phase, where the combined order data was used to produce a *probability of fraud*. The system gathers and processes the known data associated with the order and replies with “Fraud”, “Not Fraud” or “Possible Fraud”. This reply is typically returned within seconds to the e-merchant. The merchant then decides upon further action, which typically means rejecting fraudulent orders and accepting the rest. Many merchants however, choose to manually screen the “possible fraud” orders. This is normally done by temporary halting the order process for a few hours before releasing the order.



2. Strengths and Weaknesses of Static Anti Fraud Systems

Today, many existing AFSs rely on detecting fraudulent behaviour. When the accumulated fraudulent “traits” reach above a certain level, the order is regarded as fraud. This boils down to what the AFS considers to be a fraudulent behaviour. The architects of these systems perceive the total set of expected orders to be in the category “good”, “suspicious” and “fraud”. The assumption is also – and this is important – that there is a linear scale ranging from good to bad. This figure illustrates the situation:

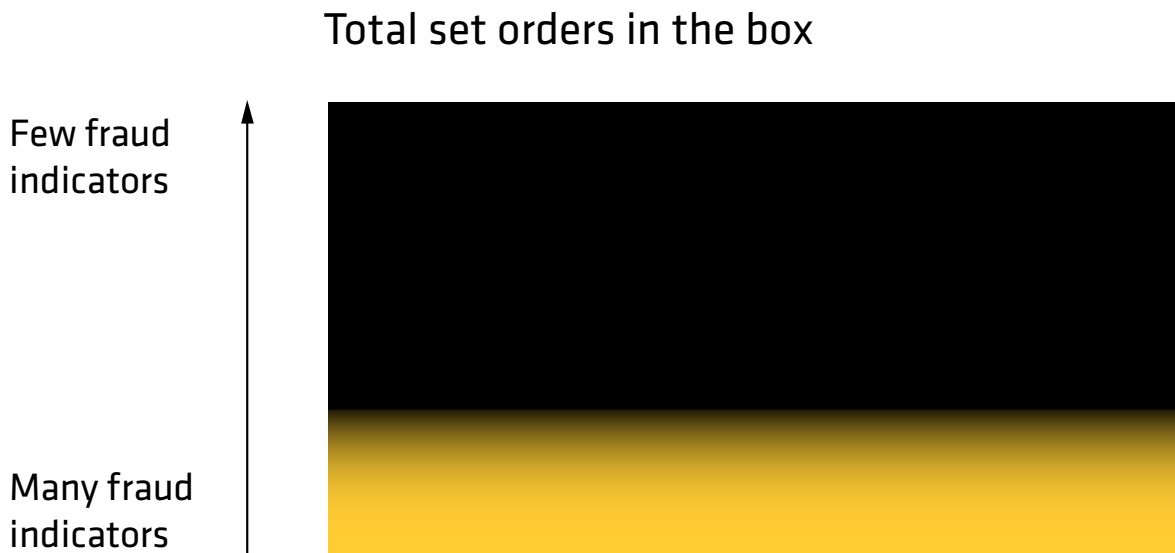


Figure 1: The black section indicates orders that have no fraudulent indicators. The yellow part has one or several fraudulent indicators. There is an intermediate section where black turns to yellow, representing few indicators or indicators that have low significance.



It is now a simple matter of applying a scale to the system to create a cut-off point. This point will typically be placed so that all or almost all of the orders in the yellow part will be rejected. The user of the system is often offered the choice of increasing or decreasing the cut-off point, depending on the merchant's risk appetite. A merchant prioritising security will typically set the point to exclude all of the orange part. In this process the merchant will reject orders that were probably non-fraudulent. This is deemed an acceptable trade off. To illustrate this, the merchant's cut off point would look like this:

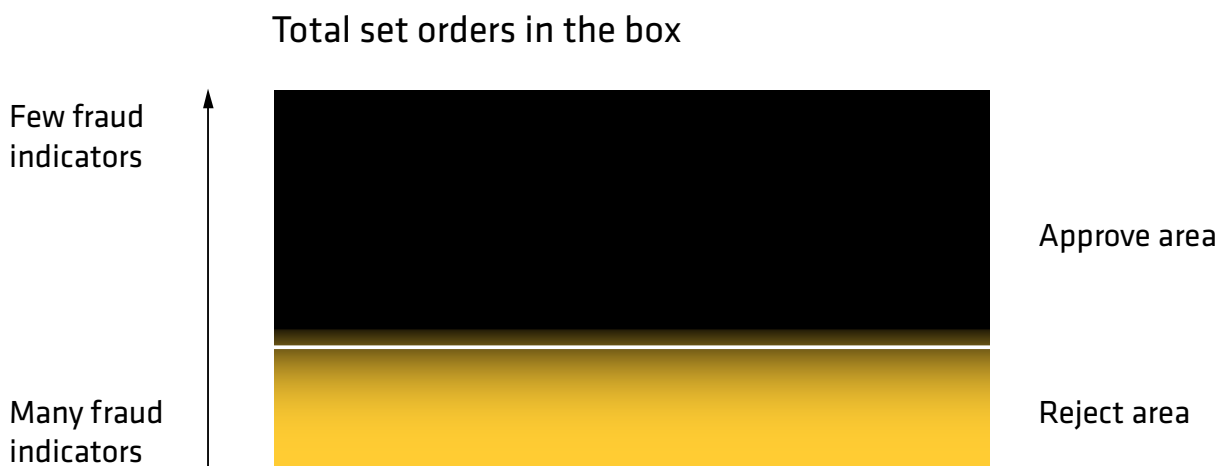


Figure 2: The merchant has chosen a threshold for the system, rejecting all orders in the "Reject Area". The threshold can be altered according to the user's wish.

If the AFS is good at detecting and finding the correlation between fraudulent indicators and true fraud, then the merchant will benefit from not accepting these.

The True Situation for E-Business Merchants

While the above example seems to offer good protection from fraud, it fails to explain the true situation in today's e-commerce environment. The truth is that today, consumers are more geographically mobile and the things they buy tend to be complex, intangible services. For a small merchant selling books and CDs to domestic customers this is not a problem. But for a large merchant offering a wide range of products and services to international customers the situation is totally different. For an Internet Payment Service Provider or an Acquiring bank, the problem is furthermore aggravated.

International customers are buying different products and they all have unique purchasing patterns. An Internet gambler in a foreign country will typically place lots of small orders in a short time frame, often at off-business hours. (The customer uses his or her payment card to top up the gambling account as the game proceeds). This kind of behaviour significantly



deviates from the book and CD merchant who typically receives one or two orders each month per customer, often within business hours or early evening.

The Internet has created new markets for services that few expected. A striking example of this is the international poker sites. Another emerging market is the online gaming sites, often involving hundreds of thousands players online. Customers are travelling more, and shop more on the Internet while abroad. IP telephony is also a fast expanding market that challenges everything that static AFS offer. The trade mark of many of these services is that they can be bought and sold on the Internet too, making them profitable for fraudsters.

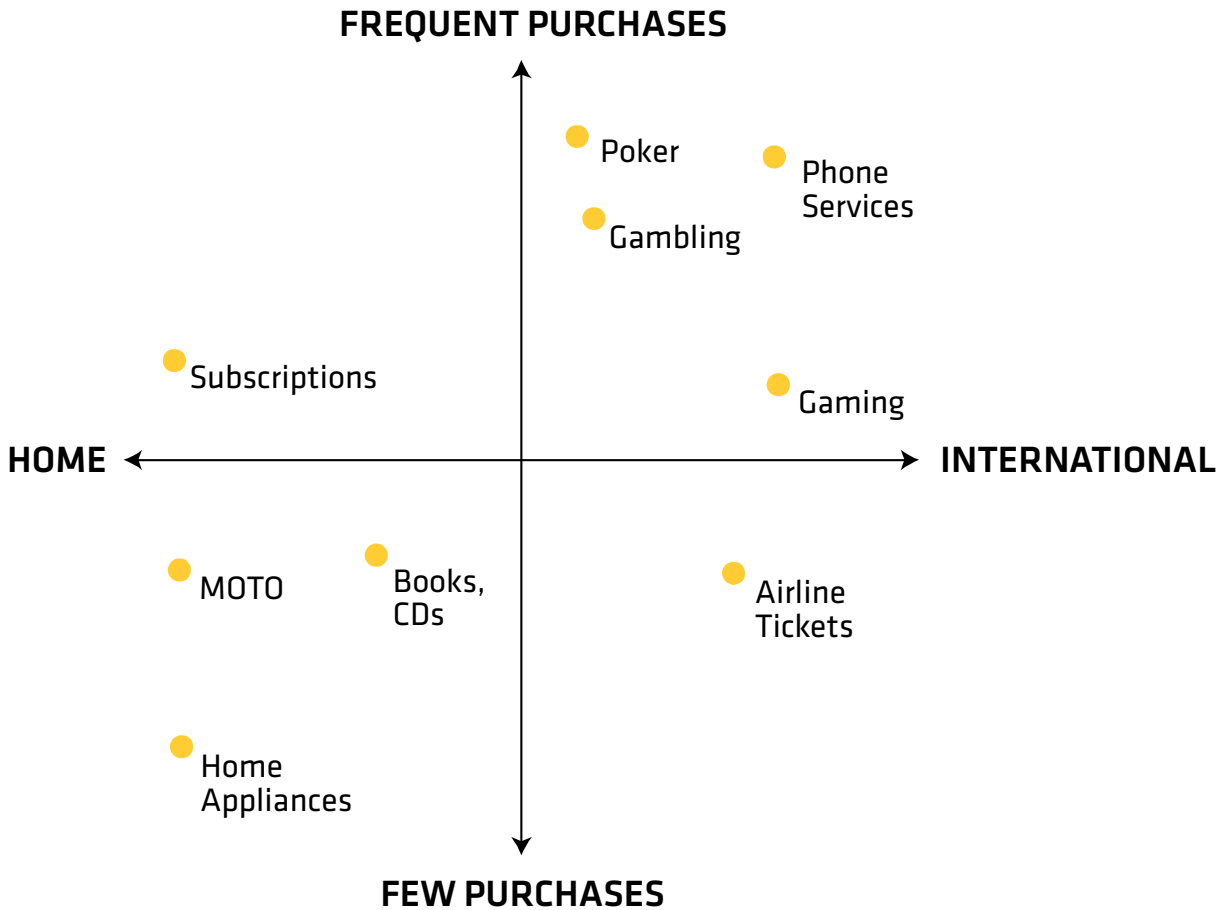


Figure 7: An analysis of different customer categories. Gaming and telephone services typically distinguish themselves as their customers place many orders in a short time frame and are geographically dispersed.

The Disadvantages of Using a Static System

An acquiring bank using a static Anti Fraud System can expect the following scoring outcome for four different customer categories:

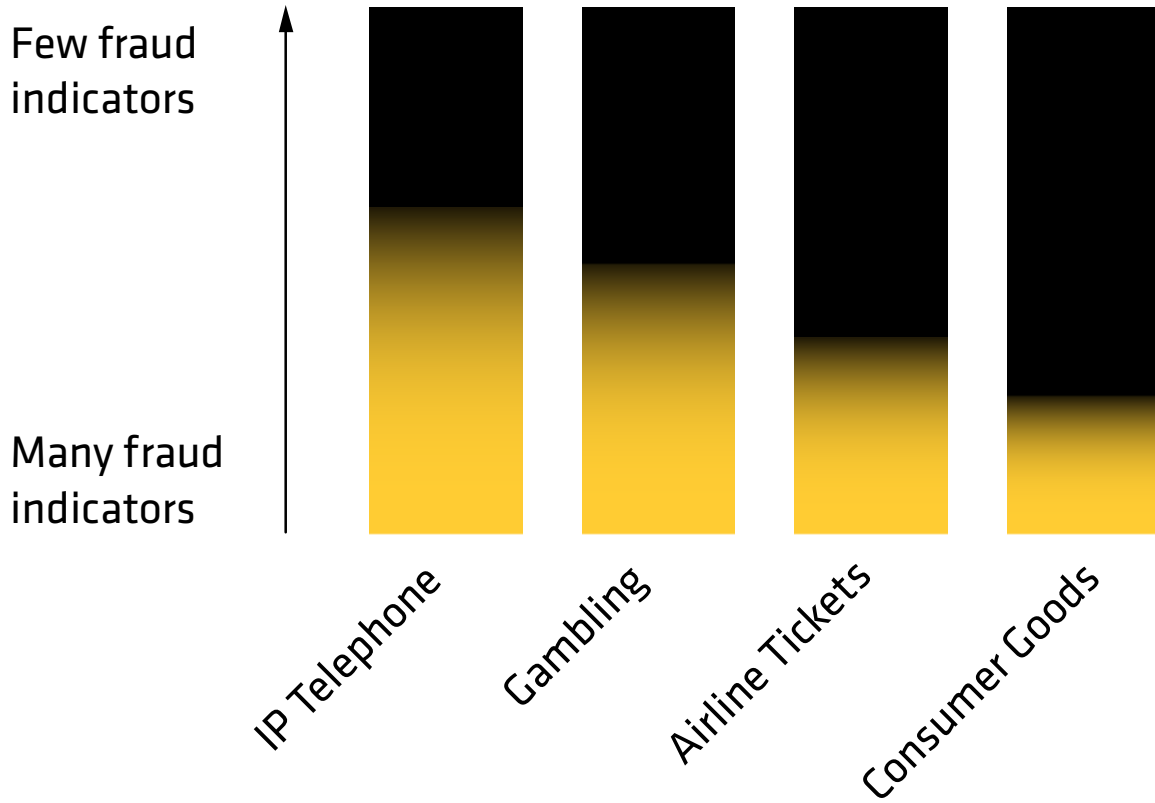


Figure 4: Four different fraud indicator outcomes caused by different customer behaviour using a Static Anti Fraud System.

Each category represents different risk, and subsequently more fraudulent indicators. The challenge is obvious: where do you set the threshold? Too strict, and too many good orders will be rejected. Too slack, and the merchant will suffer a high charge back rate due to fraud.



Figure 5: This AFS user has chosen a middle point (white line). By accepting a high rate of chargebacks for the high risk customers (yellow area above the bar) the merchant will suffer very few charge backs for the other customer categories. However, the trade off is a large amount of lost sales due to excessive order rejections.

It is apparent that a static Anti Fraud System does not satisfy the business needs of Payment Service Providers or Acquiring Banks. Chargebacks must be kept at a minimum, but the cost of achieving this is increasing as more and more genuine orders have to be turned down. Not only does the company lose revenue, it also creates bad publicity for the company as customers trying to place orders will receive a “Your order has been rejected” message. These customers will shop at a competitor’s web shop instead. Furthermore, they will share their opinion about that merchant’s web site with their friends.



3. New Markets – New Anti Fraud Systems

Introducing the SAMPORT ZEUS® With Dynamic Filters

Samport Payment Services AB now introduces its Anti Fraud System for Acquiring banks and Payment Service Providers: the SAMPORT ZEUS with Dynamic Filters. This system addresses the problem with diverse customer categories by assigning each customer category to a designated fraud filter. This means that the SAMPORT ZEUS software will be tuned to certain customer behaviour. Samport Payment Services AB has accumulated and analysed hundreds of thousands of transactions in close co-operation with large international acquiring banks (see *Figure 3*). The result is a unique insight in customer behaviour for different industries, combined with known fraudulent behaviour. This means that the SAMPORT ZEUS System can simultaneously accept and reject orders from a wide array of customers, without the shortcomings of a static system, i.e. accepting fraud and rejecting good orders.

Whenever a new e-commerce merchant signs up for an acquiring bank or a PSP, that merchant is assigned filter entry in the SAMPORT ZEUS. This entry or filter depends on the merchant's primary business profile, the bottom line being the Merchant Category Code. Recognising the shortcomings of these codes, Samport has split some key categories and added 2-4 more categories not currently represented by the MCC's.

An acquirer using SAMPORT ZEUS will not suffer the dilemma created by obsolete/static Anti Fraud systems. The dynamic filters allow simultaneous processing of an infinite amount of merchants, using 20 unique filters. To illustrate this, the previous mentioned cut-off point has radically changed:

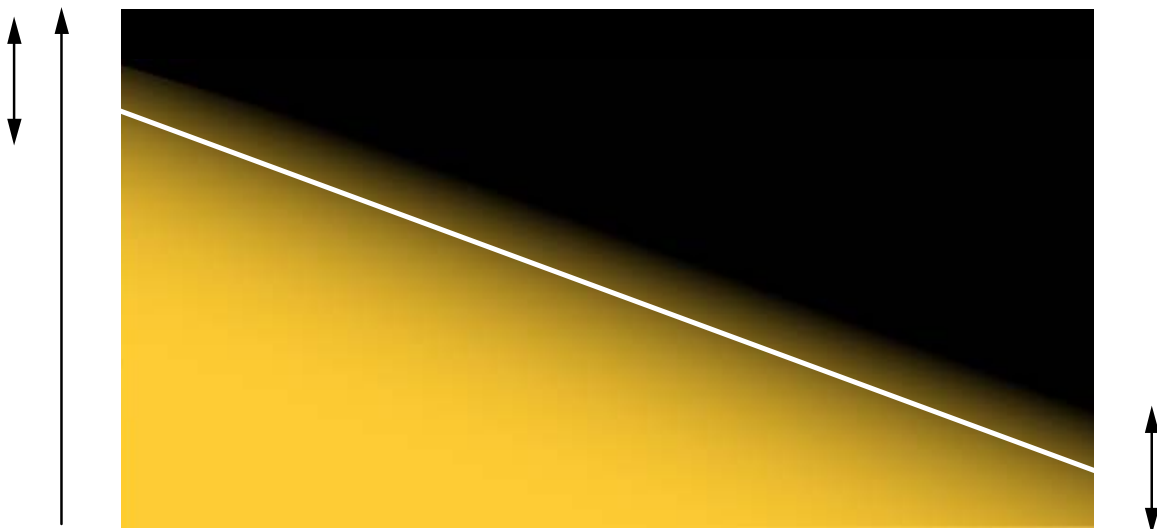
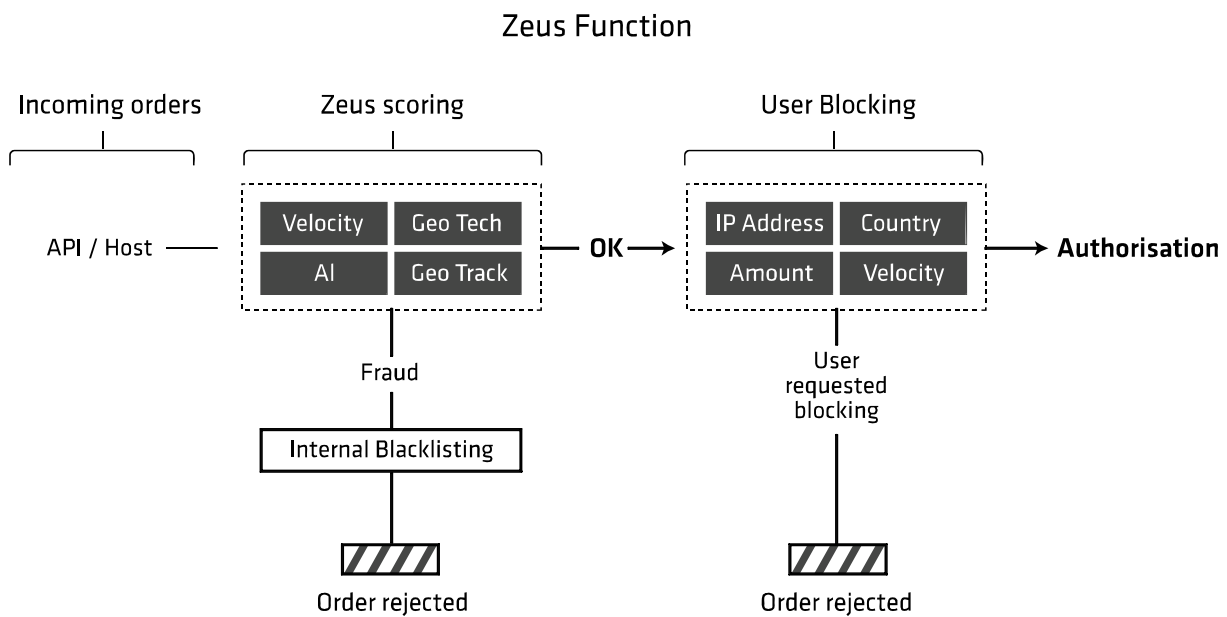


Figure 6: The tilted cut off bar represents the dynamic filters in action, effectively rejecting the yellow, fraudulent transactions whilst accepting the good orders (black). The Accept/Reject threshold can still be altered depending on the users risk appetite.



4. How does it work?

SAMPOR ZEUS is a *module based dynamic* Anti Fraud System that processes an order and produces a risk scoring within seconds. This scoring ranges from 1 to 10, with ten indicating the highest probability of fraud. This graph shows the principal sequence of events for the order flow:

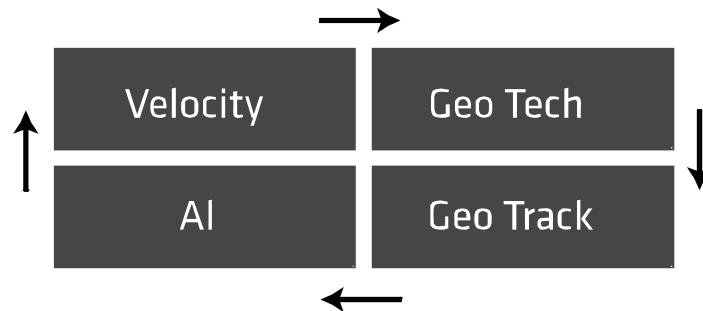


All incoming orders are processed in the Scoring section. This comprises 4-6 modules (only the four principal ones are shown). These modules simultaneously screen the order data, ranging from IP address, card issuing bank, the customer's country of residence and the product/service purchased. If one or several of the modules assigns a high scoring due to risk factors, the order will get blacklisted and rejected. The order process is then terminated.

The blocking section follows the scoring section. This is configurable to block an order if the order has one or several risk factors that the merchant considers to be undesirable. In effect this section is a straightforward "business rules" tool that allows the merchant or bank to impose a yes/no criteria for an order. Many merchants wish to block customers from certain countries or restrict the purchase amount. Furthermore, the velocity section limits the amount of times a customer is allowed to shop, typically split by 30 day's integer. The blocking section is controlled online through a web interface, allowing each end user (e-commerce merchant or acquiring bank) to directly control risk. No involvement of technical support is needed.



Zeus Scoring



The Modules and the Dynamic Interaction

The *Velocity Module* is one of the key features of the Dynamic filters system. This module is tuned to various customer buying frequencies. The module reacts to excessive amounts of orders placed during a short time frame – a typical fraudulent behaviour. This varies heavily depending on which customer category is processed. A betting or lottery site will typically experience numerous small purchases within a short time frame, compared to a site that sells home electronics. With the Dynamic Filters System, this module is pre-set accordingly, giving the betting/lottery site customers a low risk scoring in spite of the high frequency of orders.

The Geo Tech and Geo Track modules utilise the latest technology in tracing the geographical location of the end customer's computer. These two modules are particularly adept at detecting inconsistencies in the delivery address and the physical location of the buyer. A large database keeps track of every single IP address in the world, together with a cross reference post code system. Should a fraudster try to mask his or hers IP address through routing, the Geo Tech module will discover it and assign a very high risk scoring to the order, effectively rejecting it. Thanks to the Dynamic Filter System, these modules are pre-set to provide a smooth processing of international shopping sites, compared to sites that focus on domestic customers.

By far the most sophisticated obstacle to fraudsters is the Artificial Intelligence (AI) module. A fraudster has little chance of succeeding, thanks to the module's advanced behavioural interpreting coding. This has been achieved by accumulating statistics from thousands of live fraudulent transactions over a period of several years. This module also analyses the order composition. Samport Payment Services AB has developed a unique coding system for each merchant industry, making it possible to dissect the nature of the particular purchase. The code reveals if the customer bought for instance, 10 items of hardware without accessories, and how attractive these items are on the second hand market. This puts a stop to unusual purchase patterns.



5. Conclusions

Acquiring banks and payment service providers are facing a more challenging situation due to the diversity of their customer's behaviour. SAMPOR ZEUS with Dynamic Filters is the first Anti Fraud System that is designed for processing diverse customer categories. The main difference compared to a static system is that SAMPOR ZEUS recognises the need for different settings for different customer categories rather than "one size fits all". SAMPOR ZEUS capitalises on effective, high-tech solutions combined with a solid statistical analysis of today's e-commerce market.

SAMPOR ZEUS's strength is its ability to discriminate between different behaviours and apply them in the risk assessment. This means that the end-user, the merchant, is well protected against fraud and simultaneously allows genuine transactions to be completed. Some static systems are good for catching fraudsters, but the side effect can often be an excessive rejection rate. Apart from the negative customer experience and direct lost revenue, this also generates phone traffic to the merchant with customer complaints. This also adds to the combined cost of an inefficient Anti Fraud System

Together with the user web interface, the Dynamic Filters provide a highly efficient and user-friendly Anti Fraud System, configurable to suite all acquiring banks, payment service providers and merchants.

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.