



***FraudScreen.Net* Internet Fraud Protection Service**

How the FraudScreen.Net Score Works

INTRODUCTION

The Internet is a revolutionary commerce vehicle, providing an unprecedented distribution channel to retailers. However, there are risks associated with doing business on the Internet. The incidence of fraud on the Internet is much higher than for brick-and-mortar shopping venues. The anonymity of the Internet not only attracts greater fraud activity, but also the exposure of an Internet merchant on such transactions is incomparably greater than for a merchant with a physical store. The "virtual" nature of the Internet transaction means that the merchant assumes the full risk of a credit card purchase, regardless of the authorization response returned by the issuing bank. Effective and timely fraud control is necessary for managing this risk. Out of this need, *FraudScreen.Net* was born.

Going beyond standard AVS and authorization response checks, *FraudScreen.Net* provides an assessment of the fraud risk associated with each purchase over the Internet. *FraudScreen.Net* combines HNC's established expertise in credit-card fraud detection with a unique service-bureau operations environment in which it is possible use knowledge of the consumer's e-commerce activity over the entire Internet to assess the fraud risk on any given transaction. *FraudScreen.Net* uses neural networks, expert rules, and proprietary behavior profiling technology to uncover fraud patterns accurately and with minimal interference in a legitimate buyer's purchases. Typically, over 65% of a merchant's e-commerce fraud can be prevented with *FraudScreen.Net*, while impacting less than 5% of the merchant's e-commerce transactions. *FraudScreen.Net's* performance is continuously improving.

CONSUMER PROFILES

FraudScreen.Net uses neural-network-based statistical models to determine the probability of fraud on each Internet purchase. Unlike simple expert rules and linear artificial intelligence models, the HNC neural-network models analyze the "nonlinear" relationships among a consumer's spending patterns in order to predict fraud accurately. The service-bureau environment enables the models to use more than

just the consumer's behavior at a single merchant to "score" a given transaction, thus providing a more accurate risk assessment by using a more complete picture of the consumer's typical spending behavior.

Individual consumers are recognized in many different ways from the order data provided to the *FraudScreen.Net* service. Consumers are identified by the credit card they use, the IP address the order originates from, and by the billing information provided, enabling their on-line purchasing behavior to be tracked.

FRAUD SCORING

FraudScreen.Net tells merchants whether to reject or accept an order. This advice is based upon patented neural network technology developed over the last ten years. *HNC's* Fraud Data Consortium provides real world examples that are used to "teach" the neural network how to recognize fraudulent orders among legitimate orders. The *HNC* Fraud Data Consortium is the largest collection of credit card transactions in the world. Users of *FraudScreen.Net*, Falcon, and Eagle products have contributed these transactions to the Consortium over the past decade, so that *HNC* divisions can continue to develop and improve our world's leading fraud control products. Based upon the research that we have conducted with this data, we have learned more than any other company about the embedded data relationships that indicate fraudulent orders. Some of these relationships can only be derived from the kind of fraud data that *HNC* manages. Many of the relationships remain highly proprietary to *HNC*.

In order to reach a fraud assessment, *FraudScreen.Net* evaluates a large number of independent and dependent relationships among data elements:

- Email address activity. For example, has the email been used elsewhere, or has there been a change in the consumer's email address? Are the domain names and IP addresses consistent?
- Ship-to/bill-to activity. Are these consistent? Are they typical of the consumer? Is a particular address suddenly appearing in many transactions, made by different purchasers?
- Shipping Method activity. Is the shipping method selected by the consumer consistent with the consumer's typical selection, or is it uncharacteristic? What are the real-world risks associated with the shipping method? For this class of goods is next day shipping riskier than two-day delivery?
- Product purchasing pattern. Are the type and number of items being purchased typical? Is the pattern typical of this consumer? Has there been a sudden shift from soft to hard goods being purchased by the consumer? Are these easily "translatable" into cash? "Outlier" transaction amounts leading to massive, single event losses (e.g. an \$80,000 purchase) are easily identified with *FraudScreen.Net*.
- Payment Methods history. Are the payment methods typical of a single consumer? Credit Master fraud involves repeated purchase attempts with computer generated credit-card numbers.
- Work/home telephone number patterns. Are these consistent with the consumer's billing address? Is a given phone number receiving many "hits"? Is the geographic distance between the two phone numbers reasonable? Is the phone number reasonable with respect to the bill-to information?

- Hour-of-day. Is this an unusual time-of-day/day-of-week for a particular purchase by this consumer?
- Purchasing Velocity. Has the consumer made an unusually large number of purchases recently? Are the transaction amounts typical?
- Geographic location of the consumer - What are the fraud rates, as derived from HNC's 50 billion transaction consortium, that occur in the billing and ship to cities. How do these fraud rates interact with the type of goods being purchased and the other factors indicated.

MERCHANT TARGETED RISK ASSESSMENT

FraudScreen.Net renders decisions not only by considering the consumer's behavior, but also by combining that knowledge with the typical spending patterns associated with an individual merchant. Are repeated purchases over short time intervals typical of consumers at this merchant or do most consumers instead typically repeat over longer periods? Are digital or hard goods more common/risky at the merchant?

HNC has been building models to detect credit card fraud in both the on-line and brick and mortar world for 10 years. The company has over 100 man-years of development effort in building the world's leading credit card fraud detection solutions. Our experience shows that a single solution does not work for all merchants. Merchants have to sell different goods and attract different consumers. For this reason, we have built a suite of models that provide point solutions for individual industries and merchant categories. As part of our implementation process we work with the you to identify the best model or models that can be applied to the your orders.

One-size does not fit all, *HNC* delivers the best fraud detection available on the market today: *FraudScreen.Net*.