



## DATA SHEET



# VeriSign® Identity Protection (VIP) Fraud Detection Service—Data Analysis

## + Overview

VeriSign® Identity Protection (VIP) is a comprehensive suite of identity protection and authentication services that enable consumer-facing applications to provide a secure online experience for end users at a reasonable cost. VIP includes a combination of both on-premises and hosted components that can be accessed through standard network protocols for easy integration into existing Internet applications. It enables both invisible security through the VIP Fraud Detection Service and the more visible security through the VeriSign® Identity Protection (VIP) Authentication Service.

The VIP Fraud Detection Service works in real-time to detect and prevent identify theft and transaction fraud. It includes both a rules-based engine and a behavioral engine. Using rules and pattern recognition technology, the service is able to flag potentially fraudulent activities based on known and unknown types of fraud and behaviors not associated with the user. The service is designed to be simple and unobtrusive for both Web administrators and users. If the system detects a suspicious transaction, users can quickly confirm their identities using an automated system. This automated system may query the user to identify themselves further with any of the following types of credentials: a one-time password, a unique question-and-answer, email, SMS, an automated call, or a customer service call.

## + The Role of Data Analysis in Fraud Detection

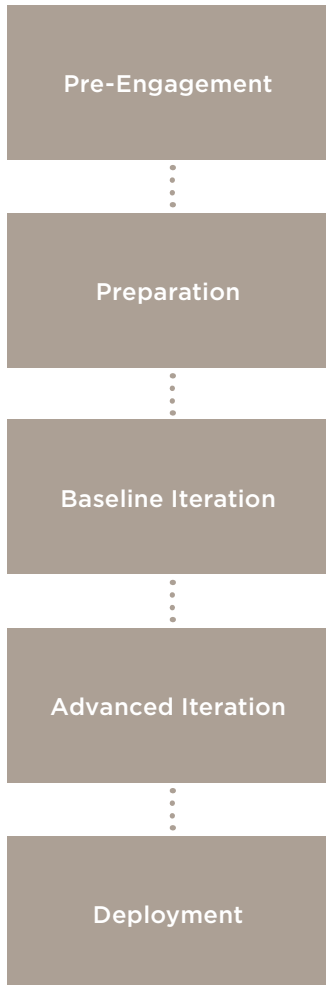
As the VIP Fraud Detection Service continues to grow, it offers more and more fraud detection methods and techniques within its fraud detection policies, which can be divided into two main groups – business rules and behavioral analysis. Business rules can be used for defining known fraudulent scenarios such as when a transaction is initiated from a high risk connection type. Such rules have the advantage of being exact and deterministic, and may be utilized from the first minute, without the need to learn from previous activity.

Behavioral rules, including machine learning techniques, can be used for identifying abnormal activity in the user's behavior, especially in cases where the abnormal activity is less obvious. These techniques are able to classify a given action as fraudulent or non-fraudulent based on the probability of the action occurring (or not occurring) in its current context.





## VIP FRAUD DETECTION SERVICE DATA ANALYSIS PROCESS



Some of these tools are relatively complex and can be optimized through customized tuning to be as efficient as possible for a given customer. The VIP Fraud Detection Service Data Analysis process is designed to tune each individual rule and the overall policy to work optimally for a given customer. Optimal settings are determined by analyzing the customer's transaction data and fraudulent activity that was detected within the customer's system. Tuning can be designed to achieve a particular outcome; for example, the system might be set to increase the fraud capture rate with a minimal intervention.

### + The VIP Fraud Detection Service Data Analysis Process

For each specific customer, some fraud detection techniques are more efficient than others, and that is where data analysis can add value. In order for the VIP Fraud Detection Service to work optimally for a given customer, it is necessary to understand which of the optional techniques are most appropriate for that customer's specific requirements. By analyzing the customer's legitimate and fraudulent data transactions, the following information is obtained:

- Which of the customer's users and transactions are processed by the system
- Which of the suggested business rules are most efficient in capturing fraud and any additional rules that can help
- What the best techniques are for identifying anomalies in user behavior patterns
- Which anomalous behavior patterns most correspond with fraudulent activity
- Whether there are any risky characteristics that can help to increase the fraud capture rate

Following the data collection, the data analysis process is initiated in phases:

**In the Pre-Engagement phase,** VeriSign determines the customer's goals and expectations of the data analysis project, along with understanding the customer's current environment and business logic.

**In the Preparation phase,** VeriSign can perform the required steps for starting the actual analysis: validate the customer's data, verifying the correctness of its structure and content; install hardware and software working environments; and prepare sample data sets as needed.

**In the Baseline iteration,** VeriSign can perform an analysis on the customer's data, using his or her current fraud detection policy (often the VIP Fraud Detection Service default policy). This can serve as a reference point for the new proposed policy later on.

**In the Advanced iteration,** based on all the knowledge accumulated up to this point, VeriSign can construct and test an optimal fraud detection policy for the customer, taking into account the customer's goals. This is the core activity in the data analysis process.

**In the Deployment phase,** VeriSign can complete all preparations that are required for deploying the newly proposed configuration. This includes a gap analysis for understanding how far the customer currently is from implementing the new policy, and a full deployment plan for filling these gaps.



## DATA SHEET

### + VeriSign as a Trusted Partner

Consumers know to use their VIP Authentication credential wherever they see the VIP logo, and that their credentials are backed by the same company that secures the Web site they do business with.

VeriSign is among the most trusted consumer brands for Internet security. Today, over 90,000 Web sites across 150 countries display the VeriSign Secured® Seal, allowing customers to confirm the identity of e-commerce sites. VeriSign's SSL solutions protect over 40 of the world's largest banks, 43 of the world's top 50 e-commerce sites, and 93 percent of Fortune 500 companies. VeriSign can better protect you from fraud and help protect your customers from identity theft.

### + Learn More

For more information about VeriSign Identity Protection, please call 650-426-5310 or email: [identityandauthenticationservices@verisign.com](mailto:identityandauthenticationservices@verisign.com).

### + About VeriSign

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

**Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.**



©2008 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the Checkmark Circle, VeriSign Secured, and other trademarks, service marks and designs are registered or unregistered trademarks of VeriSign, Inc., and its subsidiaries in the United States and foreign countries. All other trademarks are property of their respective owners.

00025788 3-27-08