



DATA SHEET

Fraud Detection – Why VeriSign?

1. Rapid & Flexible Deployment

The VeriSign® Fraud Detection Service (FDS) is capable of running in both “Zero Integration” and “Real Time Intervention” modes, allowing for extreme flexibility and a zero-footprint installation.

Zero Integration Deployment Mode for Instant FFIEC Compliance

FDS can use transaction log files or RDBMS entries in near real-time, requiring no changes to the web application and allowing for a true zero integration implementation.

FDS comes pre-configured with the ability to read industry standard web and application server log files. The Fraud Detection Service automatically detects new entries to the log files and reads only the incremental changes, allowing for high performance when reading from large transaction repositories. All FDS functionality is available, including complete protection by both the behavior and rule engines. Transactions identified as being suspicious for fraud generate real-time alerts via email, SMS or phone, and are available for instant viewing over the FDS web portal and on-line reports. This implementation mode allows for a no-risk implementation while providing FFIEC compliance and industry leading fraud protection.

Real-Time Intervention Deployment Mode for Tighter Application Integration

FDS can also be implemented in a true real-time environment with enhanced bi-directional functionality.

This deployment mode includes the VeriSign® Identity Verification Service, allowing for both in-band and out-of-band user interaction to verify the identity and intent of a user when an anomalous transaction is discovered. Integration is accomplished by using out of the box Java and .NET adapters to tie into the web application. For both Java and .NET implementations, minimal integration effort is required. FDS is able to automatically collect transaction and session information used in the fraud detection process. Integration is also available to the Fraud Detection Service over standard open API's, including support for web-services via SOAP and XML/RPC.

2. Intelligent Anomaly Detection

Unsupervised Learning

The VeriSign approach for discovering fraudulent behavior is based on the concept of unsupervised learning. The system itself is required to decide which of a user's actions correspond to his natural behavior and which are exceptional, without any assistance.



Where it all comes together.™

With the help of unique clustering algorithms, the VeriSign Fraud Detection System is able to detect suspicious activity within the data in a non-prescriptive way. While the system observes the user's transactions, it discovers common behavior patterns by grouping similar transactions together. For example, if a user tends to perform his financial activity from work on working days and from home during the week-ends, two clusters will be automatically formed, characterizing this user's common behavior during both types of periods. This approach minimizes false positives because it molds to each user's unique behavior, and maximizes fraud detection due to its capability to spot anomalous behavior down to the user level of granularity.

User Adaptive Modeling

Many fraud detection solutions overemphasize the importance of certain parameters such as machine fingerprint or IP address in order to determine if a transaction is fraudulent or not. That type of approach (i) does not capture more sophisticated fraud (e.g. fraudster moves between different machines/IPs) and (ii) generates more false positives as many legitimate users are not consistent with the machines and IPs they use.

The VeriSign FDS unique behavioral engine builds a model for each user that accurately scores whether a new transaction fits with such user's unique behavior. Where traditional solutions try to push for a one-size-fits-all, our solution automatically generates a custom model for each individual. This capability is crucial for applications with heterogeneous user bases, where there is no standardized user behavior. FDS automatically adjusts the weight associated with each transaction parameter based on how important that parameter is for that specific user (e.g. a geolocation parameter will have much more weight for a user who does not travel then for a user that travels to new places frequently). In essence, FDS is capable of painting an accurate "picture" of each individual, focusing on the behavior elements that define that person without getting distracted with other uncharacteristic traits.

In addition, information gathered from in-band and out-of-band challenge/response questions to the suspicious transactions is then used by the system to eliminate future false positives for each user, and learn what fraudulent transaction patterns look like for sharing across the enterprise.

3. Future-Proof Approach

Zero Day Attack Protection

Traditional fraud detection solutions rely on rules and IP/machine blacklists to detect a potential fraudulent transaction. These approaches cannot detect fraud attempts that are novel (therefore no rules are tripped) and originate from non-blacklisted IPs/machines. The FDS behavioral engine spots any anomalous activity, including those originated from new fraud attacks from non-blacklisted IP addresses (Zero Hour Fraud). Using state of the art clustering algorithms, VIP FDS uses characteristics of user logins—web browser type, IP address, time and date, account owner information, and other parameters—to build a profile of normal user behavior. When a transaction attempt does not match a user's normal patterns - perhaps because the transaction is from a different computer, on a different day, or in a different country - the VIP FDS system flags the transaction as suspicious, even if that transaction does not trip any rules and comes from non-blacklisted machines.

Network Intelligence

To extend the fraud visibility of our customers beyond their own network, customers will be able to link the VeriSign Fraud Detection Service to a VeriSign fraud intelligence network. The fraud intelligence network, which VeriSign intends to make available in the summer of 2006, will allow for the sharing of critical fraud data and signatures across Web sites of network members and strategic partners. This network will also leverage VeriSign's unique visibility gleaned from the operation of core Internet technologies such as SSL or DNS.

4. Comprehensive Solution

Dual Anomaly Detection

VeriSign FDS uses a unique behavioral engine in combination with a powerful rule engine to maximize fraud detection and minimize user impact. The rule engine provides a blanket of protection and policy enforcement to all users, helping enterprises address known fraud risks and business policies. The behavioral engine adds the final layer of protection, which is automatically fine tuned for each user, addressing unknown fraud attacks and eliminating unnecessary intervention.

Built-in Real-Time Intervention

For intervention, VeriSign FDS bundles a choice of built-in and easy to deploy authentication methods. This standard service allows for both in-band and out-of-band user interaction to verify the identity and intent of a user when an anomalous transaction is discovered. It includes in-band challenge/response questions and also out-of-band verification via e-mail, SMS and automated phone call (fixed or mobile).

Complete Identity Protection

VeriSign FDS is part of the VeriSign® Identity Protection (VIP) solution, a broader offering to enable online service providers to protect their customers against online identity theft. VIP implements a layered approach to identity protection by providing a comprehensive set of services enhanced by network intelligence. In addition to the fraud detection services and intelligence network described before, VIP also includes a strong authentication service and the VIP Shared Authentication Network. The strong authentication service is a flexible, easy-to-deploy two-factor authentication solution that facilitates the management of devices through an integrated life-cycle management platform. This service also includes logistics management services such as device inventory management, shipping & handling, as well as first and second level support for consumers. VIP is based on open standards defined by OATH, an industry-wide working group for authentication. These open standards allow VIP authentication to deliver an unprecedented array of credential choices for consumers, from digital certificates to smart cards to one-time-password embedded in mobile phones or dedicated tokens.

Visit us at www.Verisign.com for more information.