



WHITE PAPER

VeriSign® Identity Protection (VIP) Fraud Detection Service Stock Trading Module





CONTENTS

+ Introduction	3
+ The VeriSign Solution	3
+ The Fraud Detection Policy	4
+ Conclusion	6
+ Learn More	6
+ About VeriSign	6



Forrester forecasts 88 million retail online stock trades in 2008 and total number of U.S. online retail trades (including stocks, bonds and mutual funds) to reach 147.7 million in 2008.

—U.S. Online Trading
Forecast 2006 — 2011,
Forrester Feb 1, 2007

“The combination of configurable rules and the self-learning engine set FDS apart from its competitors.”

—Sri Balaji,
Web Solutions Security
Engineer, Addison Avenue

VeriSign® Identity Protection (VIP) Fraud Detection Service Stock Trading Module

+ Introduction

With the increasing global use of online trading by consumers, online brokerages have a pressing need to protect themselves from online fraud such as “Pump and Dump” scams. Pump and Dump scams are typically caused by fraudsters buying large quantities of penny stocks first from their own account and then from compromised or hijacked accounts. Typical penny stocks involved in such scams are low priced with high volatility, low trade volume, low market cap stocks, etc. The sudden increase in the stock trading volume causes an artificial increase in the stock price. The fraudsters then sell their own shares of the stock to make a sizable gain. Pump and Dump scams typically take only a short time to execute. Once executed, victim’s losses range from a few hundred thousand to millions of dollars. In addition, when the losses become public, this damages the reputation of the brokerages involved.

+ The VeriSign Solution

The VeriSign® Identity Protection (VIP) Fraud Detection Service (FDS) works in real time to detect and identify theft and transaction fraud. It includes both a rules-based engine and a behavioral engine. Using rules and anomaly detection 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 or security code, a unique question-and-answer, email, SMS, an automated call or a customer service call.

Fraud can be more difficult to prevent for online brokerages and trading firms than it is for other businesses because of the real-time nature of stock transactions. The VIP Fraud Detection Service now includes a Stock Trading Module for Pump and Dump to analyze stock trades in real time after the trade is placed but before it is executed. The unique behavior engine is ideally suited to monitor stock transactions and its associated fraud. The module uses four unique models to determine the risk of each trade. In the event of any anomaly or high risk transaction, the service will flag potentially fraudulent activities and can optionally intervene to validate the transaction using the standard methods such as phone, SMS, Email etc. The VIP Fraud Detection Service Stock Trading Module is the only fraud detection solution that enables online brokerages to analyze stock trades in real time and helps prevent Pump and Dump scams without adversely affecting the user experience.

KEY MODULE BENEFITS

Faster Results

Real-time analysis and detection of potentially fraudulent trades enables shortened detection, intervention and recovery times for better consumer protection.

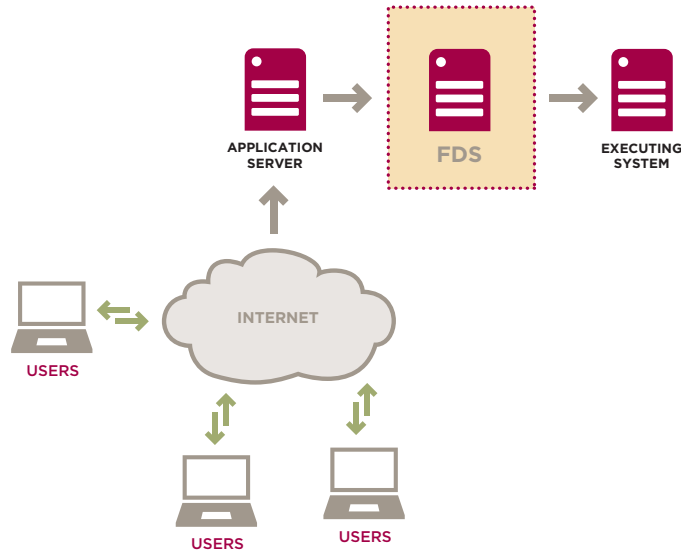
Customer Friendly

No adverse effect in user experience enables customers to trade with confidence while taking advantage of the ease and versatility of online trading.

Reliable Protection

Helps prevent online brokerages and trading firms from potentially huge losses while enhancing trust with their customers.

Figure 1: Stop Fraud Before Execution



+ The Fraud Detection Policy

The VIP FDS Stock Trading Module includes an out-of-the-box set of rules to identify common patterns of Pump and Dump fraud, immediately helping to protect users from fraud. In addition, there is a behavioral engine to analyze the history of transactions for each user and look for anomalous trading behavior. The system uses an algorithm that clusters categorical transactions based on similarity. Whenever a transaction is found that does not meet an existing historical pattern for that given user, it will be marked as suspicious.

The VIP FDS Stock Trading Module looks at four different models to assess the risk of a trade transaction.

Each model evaluates the transaction independently, returning its own risk assessment according to the unique angle it is examining. Thus each model may return a high, medium or low risk score. The module takes the input from all the individual models, and then aggregates and computes a final risk score for the transaction. The four models are:

- **Stock-oriented Model:** One fundamental purpose of the stock trading module is to identify risky and suspicious stocks. Any Pump and Dump fraud detection solution should be able to distinguish between solid and risky stocks, as it is the risky stocks that are subject to Pump and Dump scams.
- **User-oriented Model:** In the user-oriented model, the user's past trading transactions are compared against the current transaction to identify anomalies. Using behavioral analysis, trading patterns are constructed for each user using different information such as: the stock being traded on a specific stock exchange market, stock country of origin, stock market cap, stock risk level and the trade amount. The key to performing this behavioral analysis and creating the behavioral patterns is the ability to measure the similarity between any two transactions.

Different attributes are compared separately for each trade and the results are then combined to create one final similarity score. Each attribute is weighed individually using multiple algorithms and techniques specific to the attribute type and the final score takes that into account. All of this allows for the grouping of similar transactions to create clusters of similar behavior.

- **Trading-oriented Model:** The trading-oriented model identifies suspicious trading sequences. For example, if a user has performed multiple trades of the same stock in a relatively short period; then that usually does not make any sense for an individual user. Fraudsters, however, prefer to make several low-value trades to avoid detection as financial institutions may have buy-amount limits. Also the model looks for users who liquidate a large amount of stable stocks to execute a trade with risky stocks. Lastly, the model looks at ratios of trading balances to identify and track such suspicious trading sequences.
- **Network-oriented Model:** The network-oriented module looks at the connections between different entities in the network such as multiple accounts trading the same stock. Two main suspicious types are identified. The first type is when the same user performs highly suspicious trades against multiple stocks. The more trades an individual user performs in a short window, the higher the accumulated risk they will receive—which of course will be used in future transactions. The second suspicious type is when there are multiple transactions from different users involving the same stock.

Figure 2: Summary of Models

TYPE	DESCRIPTION	POTENTIAL INDICATORS
Stock-oriented suspicion factors	Measure the suitability for a stock to serve in Pump and Dump transactions	Small market cap, current vs. historical volatility, activity, exchange
User-oriented suspicion factors	Measures the likelihood that the user will trade in the type of security that might be used in a Pump and Dump activity	Prior activity trading thinly traded stocks, history of after-hours trading, number of trades per year, similarity of current trade characteristics to past trades
Trading-oriented suspicion factors	Measures if the trade in question looks like a Pump and Dump style trade	Using all available cash to purchase one security, recently liquidated a large portion of their portfolio
Network-oriented suspicion factors	Measures if multiple accounts trade the same “suspicious stock” during a very short period of time (e.g. 1-2 hours)	If this happens, it could indicate a Pump and Dump scam even when each individual trade does not raise suspicion



+ Conclusion

For online brokerages, protecting and securing against Pump and Dump scams can potentially help save hundreds to millions of dollars in losses in addition to saving the reputation of the brokerage. Given the dynamic nature of the stock market, it is imperative for a fraud detection solution to analyze and respond to such scams in real time. The VIP FDS Stock Trading Module is the only solution that enables online brokerages and trading firms to analyze stock trades in real time and help prevent Pump and Dump fraud without adversely affecting the user experience.

+ Learn More

For more information about VeriSign Identity Protection, please call 650-426-5310 or email: 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 for more information.

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

00026217 7-21-2008