Symantec™ Fraud Detection Service Description

Introduction

Symantec™ Fraud Detection Service (FDS) provides a real-time user verification and transaction monitoring system for fighting identity theft and application fraud. Rather than focusing on trying to stop the spread of false emails and websites, Symantec, through the Fraud Detection Service ("Service"), provides protection at the point where it matters most – the online site.

The system works by monitoring and learning all user and transaction behavior. Real-time transaction information including IP-based geo-location, transaction details, and user information is constantly monitored and forms the basis for the behavior models.

User sign-ins and transactions are checked in real-time against defined policies and patterns and anomalies are identified against normal behavior. When a transaction is tagged as suspicious, advanced workflow scenarios are initiated resulting in an immediate response to the fraudulent login or transaction.

Capabilities

Symantec Fraud Detection Service provides the following capabilities:

- **Real-time transaction processing engine** - User sign-ins and transactions are checked in real-time against defined policies and patterns and anomalies are identified against normal behavior. If a transaction is tagged as suspicious, an alert can immediately be sent to the company fraud group, a case can be created, or a series of automated dynamic challenge/response questions can be initiated or security codes can be sent via the Fraud Detection Service Application Programming Interface (API).

- **Self-learning anomaly detection** - User behavior is never static, and must be constantly analyzed to provide extremely accurate results when looking for anomalous transactions. Based on advanced machine learning techniques, the Service learns to adapt to the unique patterns of the user in order to accurately differentiate between valid and anomalous transactions.

- **Rule-based anomaly detection** - The Service includes a powerful rule system for adding sophisticated checks against the real-time flow of user sign-in and transaction data. No longer will data checks require custom coding or developer time to implement or make adjustments. A powerful GUI-based natural language editor is provided to quickly and painlessly implement sophisticated data checks.

- **Case Management and Reporting** - Beyond the real-time notifications of fraudulent activity, the Service provides one of the most fundamental and important ways of improving your business – the analysis and understanding of suspicious events. Case Management views can be quickly set up with detailed information about select transactions that can help you identify and understand your users and transactional environment.

- **Challenge / Response User Verification** - Both in-band and out-of-band (e.g. secret code via e-mail) User Verification is provided as part of the Symantec FDS Challenge/Response API. When an anomalous transaction is detected, multiple layers of automated challenges can be automatically initiated based on the risk that the login or transaction is fraudulent. Advanced string matching algorithms are used to reduce user entry errors. Challenges can also be sent through other optional out-of-band communication channels such as automated phone calls and SMS messages. Additional fees may be charged for these additional out-of-band challenge mechanisms as mutually agreed by Symantec and the Customer.

- **Lists and Databases** – The Service includes regularly updated Lists and Databases that provide network, financial and other data. The Network Location Database can be used to determine the geographic location from which the user is connecting to the online site. The Network Watchlist Database contains information on potential network sources of fraud (unallocated addresses, addresses used to host Phishing sites, addresses used to launch zombie attacks, etc.). Customer may use these Lists and Databases to assign risk to the user transactions that the Service is monitoring. Customer may not use these Lists and Databases as the sole and exclusive basis for denying service to any users but rather must use the Lists and Databases in conjunction with other Service rules and user behavior anomalies in order to evaluate risk and decide whether to accept or deny user transactions. These Lists and Databases are not to be used for any application other than the Symantec Fraud Detection Service. In order to maintain their effectiveness, these Lists and Databases should be updated periodically via the Symantec Fraud Intelligence Network (FIN) services, available through any of Symantec's maintenance packages ("Bronze Service", "Gold Service" and "Platinum Service").

- **ID Stamp -** This feature allows users of the Customer's web-based application to customize their login experience with a personal greeting image and a welcome text. When used together with SSL certificates, Symantec FDS risk scoring policies, and Challenge/Response mechanisms, this feature can help increase user confidence of the security and authenticity of a site. It includes a set of APIs for integration with the Customer's applications, an uploading script, a database of licensed images and a sample demonstration web application. Customers can upload their own licensed images and replace the ones that come with the service.

Service Components

The Symantec Fraud Detection Service utilizes: (i) a Symantec update service in the maintenance/support component, and (ii) certain third-party licensed software as described herein. The Service is provided under an annual, renewable subscription. Note that, unless Customers purchase the Hosted Service option, the Service incorporates Software that is developed on the Java platform and deployed on Customer's premises. Symantec discourages use of the Software independently of the Service, because satisfactory and reliable results cannot be obtained from the Software without the Service components. The Software can be integrated by the Customer in its applications (Customer application pushes transactions through either synchronous or asynchronous Web Services calls) or can be deployed without application integration (data is read from RDBMS or log files). Once data is injected into the system, transactions are sent through an anomaly engine and a policy engine.

Anomaly Engine

The anomaly engine is based on mathematical and statistical algorithms, including recent research in advanced machine learning of categorical data. The anomaly engine is used to learn user's normal behavioral patterns. As transactions arrive, they are compared against the user behavioral model and determined to be either part of a typical behavior or an outlier to normal activity. The anomaly engine is an unsupervised learning system that requires little user input.

Policy Engine

The policy engine is a set of manual business rules that define a fraudulent or anomalous condition. For example, one scenario might be a real-time check for users who log in from two disparate geographic locations within an unreasonable amount of time. Several sample rules are included with the system, and a sophisticated Web UI is available to add additional rules.

Hardware Requirements *(not applicable to Customers who purchase the Hosted Service option)*

Hardware and software requirements will vary based on criteria such as the size of the Customer's organization, numbers of external users, and the frequency and types of transactions. Customers will be responsible for acquiring and maintaining requisite hardware and software requirements (other than the Symantec Fraud Detection Service) on its premises for the deployment, maintenance and operation of the Service. For details about the hardware and software requirements, please refer to the Symantec FDSInstallation and Deployment Guide. The system is extremely scalable and additional servers can be added as usage increases. The Service may be deployed with multiple servers, including high availability. Servers can be run in single or multiple locations, providing enhanced protection in cases of infrastructure failures.

Symantec Fraud Detection Service Maintenance Packages and Customer Support

1. Overview

Symantec's support commitments are outlined below for the Bronze, Gold and Platinum levels. Effective July 12, 2010, new customers of the Symantec Fraud Detection Service must procure Platinum-level support as part of their service package. Renewing customers may choose to remain at their respective support levels as part of their service package.

2. Definitions

"Customer Administrator" means a trusted Customer employee designated by the Customer as its administrator with respect to the Symantec Fraud Detection Service.

"Response Time" means the amount of time that elapses between Customer's report of a service problem to Symantec and Symantec's response acknowledging the report and indicating that a response to the problem has been initiated.

3. Customer Support

(a) Severity Levels. The Response Times associated with Symantec's provision of Customer support to a Customer in connection with the Symantec Fraud Detection Service will be based, in part, on classification of reported problems by severity level as follows:

(i) Severity 1 (Critical Events). Severity 1 problems include any events that have a *major* impact on the operations of the system and on end users' use of the Symantec Fraud Detection Service, such as the problem types described below. A Severity 1 problem must be reported via telephone support by an appropriate Customer Administrator with immediate access to the affected system(s) and related information.

- System or application unavailability that prevents critical transactions from being processed
- Online application outages that significantly impact the online availability of the Symantec Fraud Detection Service

(ii) Severity 2 (High Importance Events). Severity 2 problems include any events (other than Severity 1 problems) that have a *moderate* impact on the operations of the system and on end users' use of the Symantec Fraud Detection Service, such as:

- Errors that disable only certain non-essential functions of the Symantec Fraud Detection Service and may result in degraded operations, including without limitation, errors that cause significant transaction processing delays
- Intermittent degradation of availability that moderately impairs the utility of the Symantec Fraud Detection Service

(iii) Severity 3 (Medium Importance Events). Severity 3 problems include any events (other than Severity 1 or 2 problems) that have a *minor* impact on the operations of the system and on end users' use of the Symantec Fraud Detection Service.

(b) Service Availability. For Bronze Service, Symantec will provide first level telephone and email support to Customer Administrator(s) 24 hours a day, 7 days a week, 52 weeks a year, for Severity 1 problems, and from 5:00 am – 6:00 pm Pacific Standard Time, Monday through Friday, 52 weeks a year for Severity 2 and 3 problems, excluding United States national holidays and Scheduled Down Time period. For Gold and Platinum Service, Symantec will provide first level telephone and email support to Customer Administrator(s) 24 hours a day, 7 days a week, 52 weeks a year for Severity 1, 2, and 3 problems. During such hours, incoming first level support calls will be answered immediately by an automated call system. Symantec will provide a call system option to speak directly to a trained Customer Support representative. 80% of the time that this option is selected (as measured on a rolling 90-day basis), Customers will speak to a trained Customer Support representative within 120 seconds of selecting that option.

(c) Response Times. Symantec's Response Times for callbacks and email support, broken out by Service type and Severity Level, are provided in Table A below.

TABLE A: Customer Support Response Time (during hours provided in Section 3(b) above)

Severity Level	***Bronze Service*** ***Response within***	***Gold Service*** ***Response within***	***Platinum Service*** ***Response within***
Severity 1 (must be initiated by telephone)	Within 1 hour	Within 1 hour	Within 30 minutes
Severity 2 (may be initiated by telephone or email)	Within 6 business hours	Within 6 hours	Within 2 hours
Severity 3 (may be initiated by telephone or email)	Next business day	Within 8 hours	Within 8 hours

(d) Problem Escalation. Severity 1 and 2 problems will be internally escalated in accordance with the procedure described below.

(i) Severity 1.

- *Hour 0 to Hour 1:* Symantec's Technical Support Manager, Escalation Management and Engineering ("EME") Manager (as may be required) are notified of the problem and are actively working on the problem.
- *Hour 1 to Hour 4:* Symantec's Director of Customer Service (Technical Support and EME) is notified and involved in the problem resolution as may be required.
- *Hour 5:* Symantec's Vice President of Customer Service is notified and involved in the problem resolution as may be required.

(ii) Severity 2.

- *Hour Zero to Hour 72:* Symantec will work to resolve the problem and will attempt to provide a solution within 72 hours after problem identification. At the Customer's explicit request and in the event that Symantec does not develop a plan within the first 72 hours after the problem is reported, for resolution of the problem within the following 10 day period, and the problem is not due to the fault of Customer, Symantec will escalate the problem in accordance with the Severity 1 escalation procedures described above.

(e) Maintenance. Bronze, Gold and Platinum Support include a maintenance plan under which Symantec will provide Software upgrades, bug-fixes, patches, error corrections and enhancements which are developed by Symantec and made available to Symantec's customers generally. SYMANTEC WILL PROVIDE SUCH MAINTENANCE PLAN AND CUSTOMER SUPPORT AS PROVIDED HEREIN ONLY FOR THE THEN CURRENT RELEASE OF THE SYMANTEC FRAUD DETECTION SERVICE OR SOFTWARE AND THE IMMEDIATELY PRECEDING RELEASE AT ANY GIVEN TIME.

(f) Hosted Service Option. As part of the Service, Symantec will, on Customer's behalf, host the Software in a highly-available configuration in one of Symantec's carrier-class data centers.

(g) Symantec Fraud Intelligence Network (FIN). Symantec will provide FIN access as part of its maintenance plan, either through a manual download or automatic download from the Symantec FDS. FIN is a mechanism for distributing Internet-level intelligence data to Symantec FDScustomers. Symantec gathers information about fraudulent activity from various sources, collates it, and provides it to our customers through the FIN. Symantec Fraud Detection Service customers may use these databases in conjunction with other Symantec FDS rules and user behavior anomalies in order to evaluate risk and decide whether to accept or deny user transactions. The information provided through the FIN cannot be used for any application other than the Symantec FDS.

(h) Service Availability for the Hosted Service Option and FIN: (i) Up Time Measurement. Up Time is calculated on a rolling 90-day basis as a percentage equal to (A) the total number of minutes in any 90-day period that Symantec's systems are available and capable of receiving and processing data from customers, divided by (B) the total number of minutes in such period. ***(ii) Up Time Percentage.*** Symantec's Up Time percentage throughout the Term will be no less than ninety-nine percent (99%) for Bronze and Gold Service, and no less than ninety-nine and one-half percent (99.5%) for Platinum Service not including Scheduled Down Time. Scheduled Down Time will not exceed four (4) hours in any single calendar week.

4. Additional Terms for Platinum Customers

(a) Customer Relationship Manager. For Platinum Service only, Symantec will designate a qualified Symantec employee to serve as Customer's Relationship Manager for the coordination of implementation activities, and management of problem resolution and escalation efforts. The Customer Relationship Manager also will be available to conduct support service reviews at Customer's request once every calendar year

(b) Reports. For Platinum Service only and upon request, Symantec will make available to Customer monthly reports detailing (for the period covered by the report) severity level classifications and current resolution status for reported problems.

SYMANTEC™ FRAUD DETECTION SERVICE ADDITIONAL TERMS AND CONDITIONS

1. DEFINITIONS

"Agreement" means the Master Services Agreement or such other agreement entered into between Symantec and Customer under which the Services set forth in this Service Description are provided by Symantec to Customer.

"Geographical Map" means the images available in the Case Management view that associate user logins and transactions with locations displayed on a geographical map using Microsoft Virtual Earth technology.

"Hosted Service Option" means the service option whereby Symantec, on behalf of the Customer, hosts the Software in one of Symantec's data centers as part of the overall Service.

"Licensed Personalized Image" means each image that is included in the database of licensed images and in the sample demonstration application that is provided by Symantec to Customer in connection with the ID Stamp functionality.

"Software" as used herein and defined in the Master Services Agreement means the Symantec Fraud Detection Software licensed to Customer hereunder.

"User" means the Customer's end-user of Customer's web-based application(s).

2. CUSTOMER'S OBLIGATION

(a) Customer Obligations. Customer is solely responsible for acquiring and maintaining requisite hardware on its premises and maintaining the security of its network and computer systems.

(b) Customer's Warranties. In addition to the express limited warranties set forth in the Agreement, Customer hereby represents and warrants to Symantec that: (i) Customer will not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any Symantec system, Software or Service; (ii) with respect to transfer of data from Customer to Symantec in connection with the Services contemplated herein, Customer has obtained all necessary consents, rights in, licenses to, and authority over all such data necessary for Customer to lawfully provide to Symantec and permit Symantec to receive and process such data as contemplated herein including, but not limited, to transferring the data Customer provides to United States and in other jurisdictions where Symantec maintains a presence for such processing; (iii) no such data does or will infringe, misappropriate, or violate any third party's privacy or Intellectual Property Right; (iv) Customer will (A) only use the information provided through the FIN to assign risk to User transactions that the Symantec Fraud Detection Service monitors; and (B) not use the Network Location Database or Network Watchlist Database as a sole and exclusive basis for denying service to any User; (v) Customer will not transfer or give access to any third party the information provided through the FIN; (vi) solely with respect to the Geographical Map feature, Customer will be responsible for compliance with the Terms of Use set forth at http://go.microsoft.com/fwlink/?LinkId=21969 and the Privacy Statement located at http://go.microsoft.com/fwlink/?LinkId=21970; and (vii) to the extent that the Service contains third-party data from Thomson Financial, the terms on the General Restrictions/Notices page set forth on http://www.thomsonfinancial.com/datause shall apply.

3. SYMANTEC'S OBLIGATIONS

(a) Installation (not applicable to Customers who purchase the Hosted Service Option). In order to optimize performance, Symantec, through its Professional Services organization, shall provide Software installation services, including major and minor upgrades, at Symantec's then-current rates pursuant to a SOW or as set forth in the applicable Services Order. If additional work is required due to unusual or particularly-complex Customer systems or requirements, Customer may purchase additional consulting hours from Symantec. Symantec shall not be responsible for providing technical support to Customers who attempt to install or upgrade the Software on its own. However, such support may be purchased from Symantec's Professional Services organization on an hourly basis, as needed.

(b) Acknowledgement of Delivery. The parties' execution of the Services Order to which this Services Description is appended shall confirm Symantec's delivery to Customer of the Symantec Fraud Detection Service Software and related documentation, and Customer's acknowledgement of receipt thereof.

(c) Limited Warranty. Symantec warrants that the Software will operate in material conformance to Symantec's published specifications during the first ninety (90) days following Customer's initial receipt of the Software ("Warranty Period"). Symantec does not warrant, however, that the Software or any portion thereof is error-free. If Customer discovers a non-conformity in the Software during the Warranty Period, Customer shall submit to Symantec a written report describing the non-conformity in sufficient detail to permit Symantec to reproduce such non-conformity. Upon confirmation by Symantec that the reported non-conformity has been reproduced and confirmed to be such by Symantec, Symantec will use reasonable efforts to, at its option, (i) correct the non-conformity; (ii) provide a work around or software patch (collectively "Fixes"); or (iii) replace the Software. If Symantec determines that none of these alternatives is reasonably available, upon Customer's request Symantec shall refund any license fees paid for the affected Software and accept its return. All Fixes provided by Symantec shall constitute Software as defined hereunder, as applicable, and shall be governed by the terms hereof. This warranty shall not apply to any non-conformity caused by any unauthorized modification to the Software or by Customer's failure to incorporate any Fixes provided by Symantec. This warranty applies only to the initial delivery of the Software. Fixes are provided with a limited warranty of thirty (30) days from receipt of such Fix or for the remainder of the initial Warranty Period, whichever is greater. The foregoing express warranties are in lieu of all liabilities or obligations on the part of Symantec. CUSTOMER'S SOLE REMEDY FOR BREACH OF WARRANTY SHALL BE A CORRECTION, FIX OR REFUND AS SET FORTH IN THIS SECTION.

(d) Disclaimer of Warranty. NEITHER SYMANTEC OR ITS SUPPLIERS WARRANT THAT THE PROVISION OF THE SERVICE WILL BE UNINTERRUPTED, ERROR FREE, TIMELY, COMPLETE OR ACCURATE, NOR DO THEY MAKE ANY WARRANTIES AS TO THE RESULTS TO BE OBTAINED FROM USE OF THE SAME OR TO THE ACCURACY OF ANY LICENSED PERSONALIZED IMAGE. USE OF THE SERVICE AND RELIANCE THEREON IS AT CUSTOMER'S SOLE RISK. IN NO EVENT WILL SYMANTEC OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION DIRECT OR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, LOSSES OR EXPENSES ARISING IN CONNECTION WITH THE SERVICE EVEN IF ADVISED OF THE POSSIBILITY OF SUCH.

4. EFFECT OF TERMINATION OF SERVICES

In the event of a termination of the Services contemplated herein for any reason, (i) Customer will immediately cease use of the Services and Software, (ii) the rights to use the Services and any related third-party software or other components will immediately terminate, (iii) Customer will permanently delete any software related to the provision of the Services, the Network Location Database, and the Network Watchlist Database from any storage media upon which such software is stored, and (iv) neither party shall be relieved of obligations or liabilities which accrued prior to the date of termination.

5. AUDIT RIGHTS

Not more than twice a year, Symantec may audit and inspect, at its own expense, Customer's utilization of the Services contemplated in this Service Description in order to ensure compliance with the terms herein, the Services Order and the Agreement. Any such audit will be conducted during Customer's normal business hours upon reasonable written notice to Customer and will not unreasonably interfere with Customer's business activities. Customer shall reasonably cooperate with Symantec in connection with any such audit. If the audit reveals that Customer has underpaid fees to Symantec, such underpaid fees shall be immediately due and payable by Customer.