

Infinitem E-Payment 2.2 Enterprise Edition White Paper

**Prepared by
Ho Ching Wee**

Nature
Private & Confidential

© Copyright 2005, Office Connect Sdn Bhd. All rights reserved.

Printed 20 April, 2005

Copyright Notice

This document, software and the concept described in it are copyrighted. Under the copyright laws, neither this document nor this software may be copied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written authorization of Office Connect Sdn Bhd.

1 Infinitium E-Payment PPS 2.2

The Infinitium E-Payment PAYMENT POS Server version 2.2 [PPS] is a payment server product designed for merchants and enterprises to enable them to provide a comprehensive online payment capability for their business transactions. PPS provides all the online payment functions required by a merchant for authorizing and settling credit cards, debit cards, private label cards, e-debit and other payment modes depending on the adaptors purchased.

The PPS may be interfaced to any merchant application by integrating the payment API provided with the merchant application. The PPS supports both hosted and non-hosted merchant environments. The PPS has optional payment plug-ins to handle virtual world payment protocols such as SSL, Visa's 3D Secure and MasterCard's SPA-UCAF. The PPS also supports multiple acquirers with slots for multiple adaptors that connect to various different payment modes such as e-debit, e-purse, MEPS cash, ATM, e-pos, MEPS FPX and etc.

Embedded within the PPS is an optional add-on plug-in, Fraud Detection Server (FDS) to help online merchants to identify potential fraud behavior and flag down irregular transactions that violates the merchant fraud parameter and sensitivity settings.

1.1 Market Opportunity

PPS overcomes many of the barriers faced by merchants. The benefits for the merchant of providing e-commerce services to customers are substantial, provided the merchant can manage the complexity, operations, security, and deployment issues both efficiently and cost-effectively.

Implementation: PPS provides Application Program Interfaces and Software Development Kits for merchant to integrate PPS into existing legacy systems. While other POS applications may require the merchant to host the entire application that handles transaction request information between a customer's electronic wallet and a financial payment gateway, PPS allows the merchant to securely link between a storefront adapter and a server-based PPS engine. This configuration eliminates the need for the merchant to become proficient in hosting and managing Internet payment systems or managing operation center support functions.

Security: The PPS has several security features that allow merchants to conduct secure multi-channel commerce. The product supports 128 bit SSL and standard secure customer authentication protocols such as Visa's 3D Secure and MasterCard's SPA-UCAF. The product also has a feature to authenticate the IP address of the client applications that request for payment services ensuring that only authorized client applications are able to gain access to the service. Furthermore, for credit card transactions, the credit card numbers are stored encrypted in the database to prevent misuse of the number.

Flexibility: Infinitium E-Pay PPS supports a wide range of payment transactions such as Authorization, Sale, Capture, Refund, Reversals and Batch Settlement to fit different business process flows. In addition all the transactions are accessible by a simple API as well as via a browser based User Interface allowing for several modes of operation viz. automatic, manual or both. For instance, enterprises may perform only order taking on their web stores, while outsourcing their ecommerce fulfillment functions

Compliance: PPS is developed with the emerging payment standards in mind. PPS supports both Visa's 3D Secure and Mastercard SPA-UCAF standards. In addition, Infinitium's strong in-house R&D team and innovative support ensures that the product stays relevant in today's dynamic world. In addition, Infinitium E-Pay PPS solution has been proven and tested to integrate with payment gateways around Asia.

1.2 Compelling Reasons for PPS 2.0

Efficient Implementation

Simple installation
Wide range of configuration options
Comprehensive storefront integration abilities

Scalability

Scalable to support numerous merchants, whether they are locally hosted or remotely distributed
Scalable to support large volumes of transactions
Scalable to support multiple acquiring banks
Scalable to support multiple payment adaptors for different payment modes

Versatile Payment Platform

Supports various payment format and mechanisms via Payment Adaptor in one common platform

- ISO Adaptors for E-POS bank card
- SSL Adaptors for Credit card and Debit card
- HTTPS Adaptors for Interbank e-Debit (FPX by MEPS)
- Phone Adaptors for CTI-based PABX Phone Credit Card
- WAP Adaptors for WAP and GRPS Credit Card
- SMS Adaptors for SMS Credit Card
- MPI Adaptors for 3D Secure and SPA-UCAF
- Batch Adaptors for off-line transactions such as MEPS Cash and e-purse

Centralized Administration and Control

Centralized administration and control
Extensive operational control to support mainstream business processes
Maintains account and transaction information

Reduced Deployment and Support Costs

Wide range of Standardized Payment Modes

Support for SSL payment transactions and provides a smooth and logical transition from SET

Support for ISO based payment transactions such as E-POS bankcard

Support for HTTPS based payment transactions such as e-debit (FPX)

Support for WAP, SMS, Phone based of credit card transactions

Support for offline payment transaction such as MEPS Cash and TouchNGo

1.3 Business Requirements

PPS is designed to satisfy the following business requirements:

- POS Functionality
- Integration
- Multiple merchant administrations
- Multiple acquiring banks
- Supports for multiple payment adaptors to manage various payment modes
- Rapid Deployment of payment modes
- Operator and individual admin module
- Customizable and extensible
- Payment System Independence
- Shopping Cart System Independence
- Payment Server Location Independence
- SSL Ready
- 3D Secure/ SPA-UCAF Ready
- Ease of Merchant Administration
- Global-ready

1.3.1 Integration

PPS provides simple methods for merchant to integrate PPS into existing legacy systems and operations center environments.

Benefit:

PPS allows our partners and their clients to leverage their existing technology investment.

1.3.2 Rapid Deployment Of Merchants

PPS allows merchant to quickly deploy and set up for payment processing over open networks, eliminating the requirement that merchants no spend hours of unproductive time doing custom programming and configuration to get a commerce application up and running.

Benefit:

PPS provides a simple, secure, and standard solution that allows merchants to easily integrate PPS client component into their merchant storefront.

1.3.3 Payment System Independence

PPS takes a payment independent approach when accepting transactions at the merchant site. Version 2.0 by default comes with the SSL Adaptor to support SSL transactions on the front-end with ready support for Visa 3D Secure by default. In addition, other types of Payment Adaptors can be added as and when different payment modes are required. Some of other payment modes include e-debit, e-purse, e-POS, phone-based credit card, SMS based credit card etc.

Benefit:

PPS platform enables merchants to support any payment transaction type in a single integrated secure solution.

1.3.4 Shopping Cart System Independence

PPS is independence of the shopping cart system of the merchants.

Benefit:

An open and independent system ensures that a merchant can support any form of payment that a consumer might be using (e.g. Open Trading Protocol).

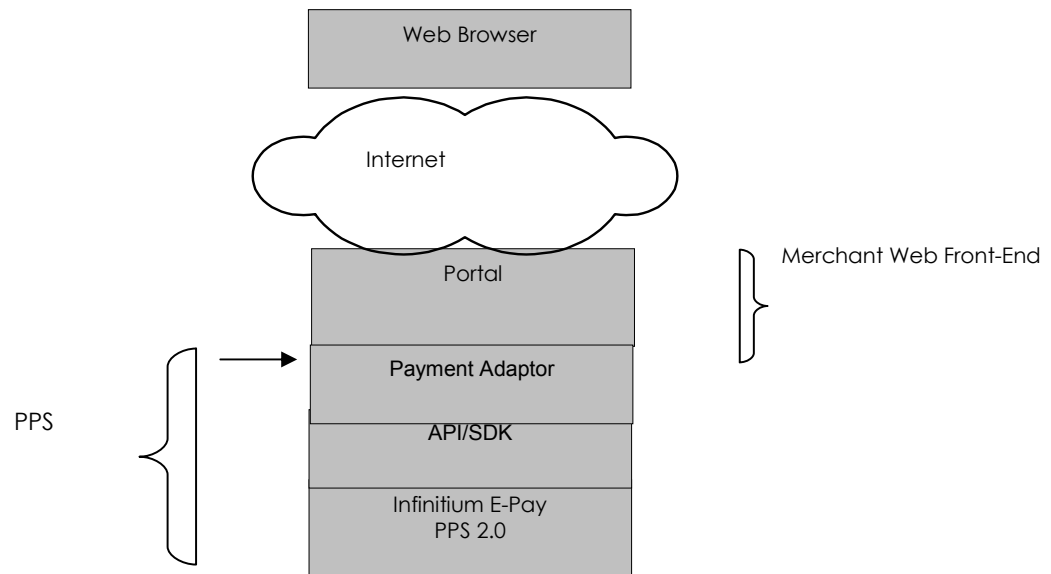
1.3.5 Ease Of Merchant Administration

PPS makes it easy for operator to control the accounts by centralizing the operator administration module. However, for multi-merchants environment, every merchant has their very own merchant administration modules This enables the merchants to manage their own e-payment information without releasing sensitive information to other competitive merchants.

2 Technical Architecture

2.1 Application Architecture

This section presents a general overview of the architecture of PPS.



2.1.1 Payment Server

PPS resides on a centralized server. It performs all associated payment transactional operations, supports high numbers of customers

2.1.2 Merchant Administration Manager

The Merchant Administration Manager consists of HTML templates and application logic that provide a web interface to several PPS features. The Merchant Administration Manager is used to:

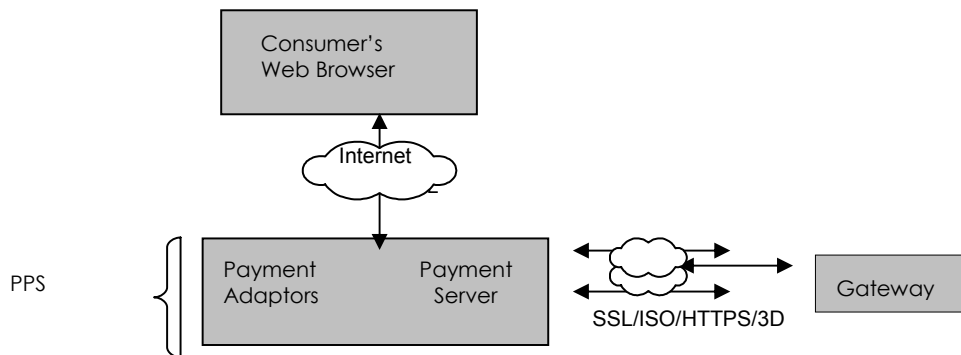
- Configure the acquirer's URLs, ports, and database
- Add or delete merchants, configure and monitor the status of current merchants
- Manually process batch activity and transaction activity

In addition, respective merchant can use a browser to interact with PPS. The merchant uses the browser to interact with the payment server much as he would use a GUI to interact with a terminal system. The merchant administration tool allows the merchant to change (depends on the access control provided by the administrator) configuration data, view

transactions, select transactions for capture, reversal, or credit, and open or close batches. In addition, the administration tool enables the merchant to view their very own transaction and settlement reports.

2.2 Payment System Architecture

This section presents a general overview of the architecture of Payment System incorporating PPS



2.2.1 Cardholder Software

An Internet browser supporting the HTML, HTTP, and SSL standards.

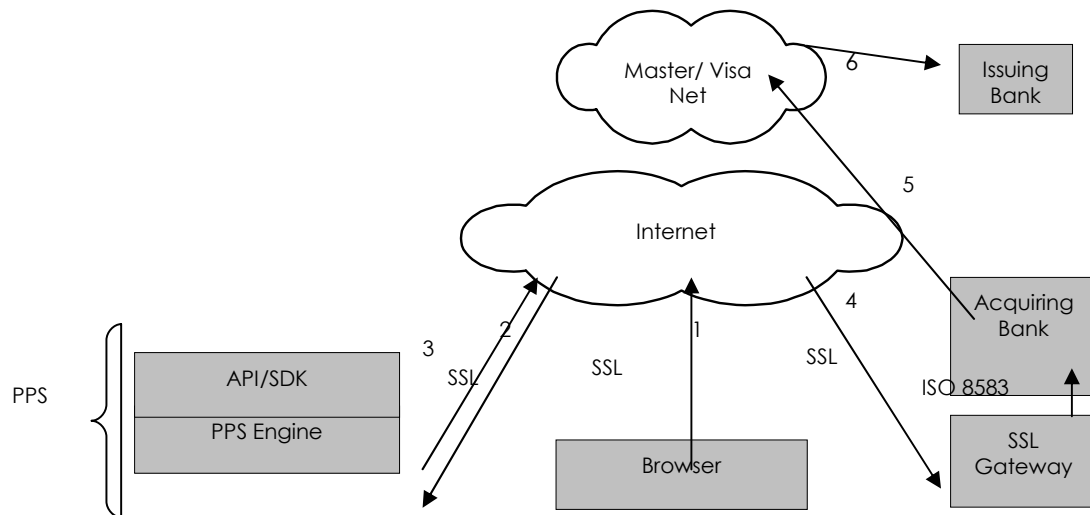
2.2.2 Merchant Administration Tool

Each merchant uses the browser to interact with PPS as much as he would use a GUI to interact with a POS terminal system. The merchant administration tool allows the merchant to change certain configuration data, view transactions, select transactions for capture, reversal, or credit, and open or close batches. In addition, this tool enables the merchants to view their own transaction and settlement reports.

2.3 PPS Payment Processing

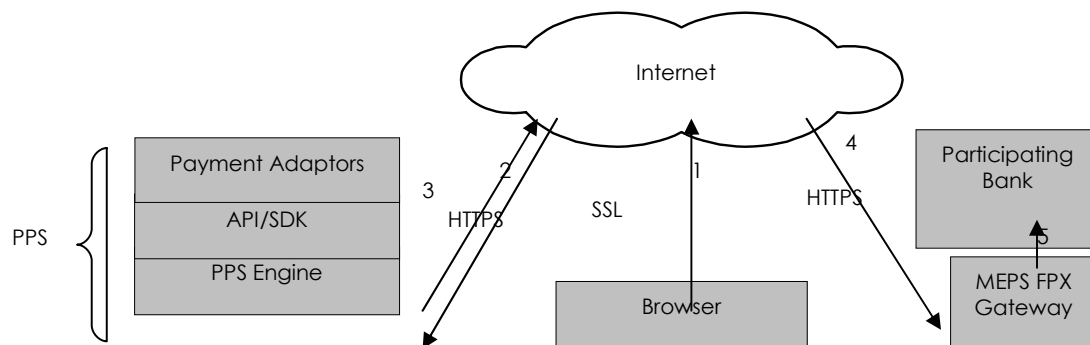
PPS takes a payment independent approach when accepting transactions at the merchant site. Version 2.0 by default comes with the SSL Adaptor that provides support for SSL transactions. Other Payment Adaptors to support other payment modes are also available and can be added as and when required.

2.3.1 SSL Payment Processing



- The cardholder is shopping at merchant Storefront using his web browser over the Internet
- The cardholder chooses an item
- The cardholder will be required to fill in credit card number and expiry date
- At this point, the normal SSL protocol messages, message flows, and processing take place between PPS and the payment gateway
- Once the SSL transaction is complete, control of the process is again returned to the merchant's storefront application in order for the transaction to be completed between the merchant and the cardholder.

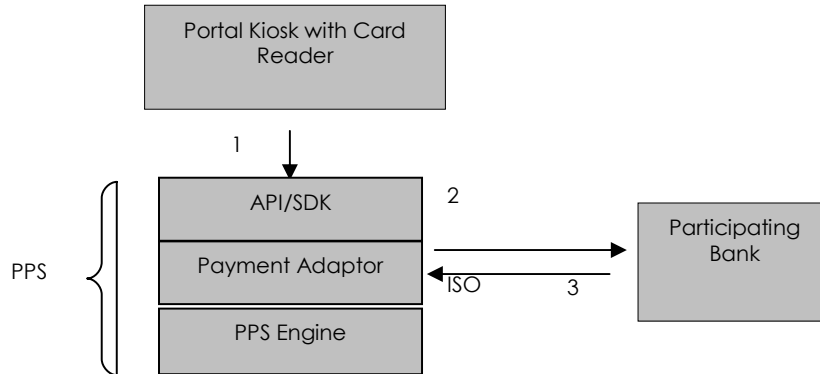
2.3.2 E-Debit Processing(Debit Current/Saving Account)



- The buyer is shopping at the Merchant Storefront using his web browser over the Internet
- The buyer purchases an item and decides to pay by using e-debit from his/her bank account. The buyer chooses E-Debit Payment Option and will be redirected to his/her online banking screen (eg. Maybank2u)
- The buyer will be required to login into their Internet Banking account

- The buyer will need to validate balance and direct debit account to the seller
- Issuing bank via FPX informs buyer of successful transaction. FPX sends notification to PPS to update seller on successful transaction.
- PPS captures the transaction status and updates the merchant Storefront

2.3.3 E-POS (Bankcard Debit)



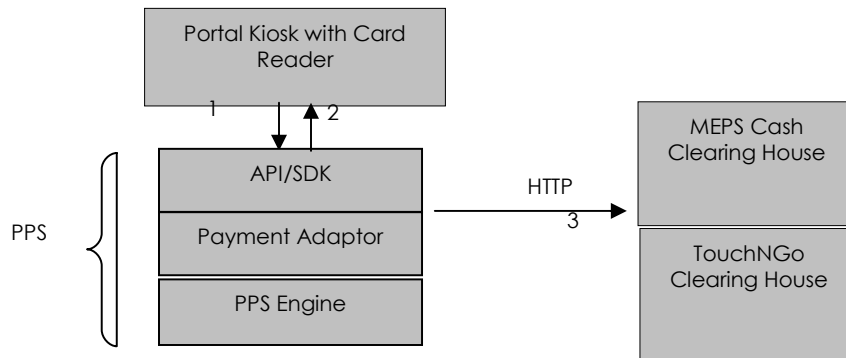
The buyer is shopping at the Merchant Kiosk. Buyer decides to pay for the services with E-POS (ATM Bankcard). Buyer inserts the ATM bankcard (e.g. Maybank Kawanku) into the E-POS reader.

The information will be captured by the PPS 2.0 and will be submitted to participating bank via ISO Adaptor for real-time processing.

Participating Bank replies with transaction status.

PPS 2.0 captures the transaction status and updates the merchant portal Storefront

2.3.4 E-Purse Debit (MEPS Cash and TouchNGo)



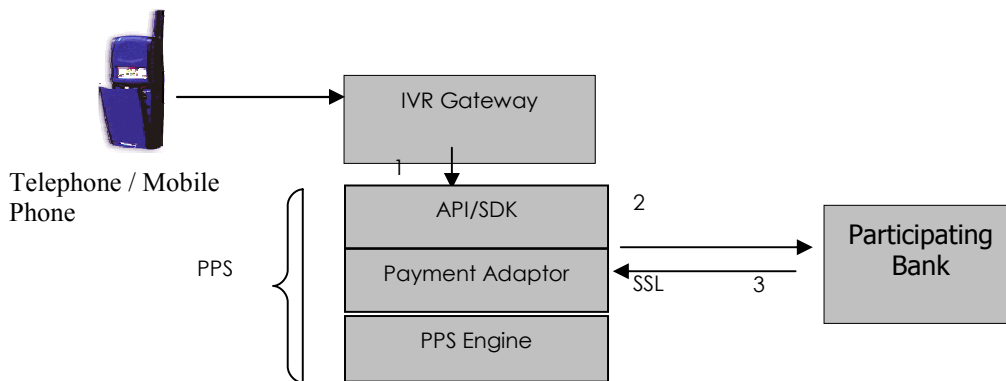
The buyer is shopping at the Merchant Kiosk. Buyer decides to pay for the services with E-Purse (MEPS Cash / TouchNGO / MyKAD).

Buyer inserts/swipe its E-Purse Card into the reader. The reader will deduct the credit in the e-purse. All the transaction information will be captured by the PPS and submit to respective clearing house via Batch Adaptor for batch updating at the back-end server.

2.3.5 IVR Credit Card

Infinitem E-Pay PPS 2.0 can also support Credit Card transactions over the Telephone for MOTO based transactions. Once connected to the IVR gateway, user will be able to select the IVR voice menu to initiate the Credit Card Payment process. User will be able to punch in their 16 digits card number along with other details such as expiry date and CVC using the telephone keypad

The IVR Gateway will be able to convert those information details using DTMF and forward the information to PPS with encryption.



The information will be decrypted will be captured by PPS 2.0 and submit to participating bank via IVR Adaptor for real-time processing.

Participating Bank replies with transaction status.

PPS captures the transaction status and updates the merchant portal Storefront

3 Rich Functionality For Every Business Need

Our R&D team will continuously work on new improvement and enhancement of the product with value added features while striving to maintain backward compatibility of its releases.

3.1 Features And Functionalities

Operator Administration

- Create and Administer Users
- Create and Administer Merchants
- Create and Administer Acquirers
- Create and Manage Batch Close Scheduler
- View Batch and Transaction Summary
- View Transaction Audit Logs
- View Transaction Audit Log By user
- Printing of Reports

Merchant Administration

- Create and Administer Users
- Create and Administer Acquirers
- Create and Manage Batch Close Scheduler
- View Batch and Transaction Summary
- View Transaction Audit Logs
- View Transaction Audit Log By user
- Printing of Reports

Payment Functions

- Authorization
- Sale
- Capture
- Credit (or Refund) of Captured Transactions
- Sale/Auth/Credit/Capture Reversals (or Voids)
- Batch Close
- Batch Reports by date
- Report transactions by Batch number, Transaction type, date, date range
- View User Transaction Audit Logs
- Printing of Reports

Security Support

- VISA 3D Secure Merchant Plug In
- IP Authentication of merchant web server (configurable)
- CVV2/CVC2/CID capable
- Configuration of User Access Rights
- SSL for host communications

Supported Host and Communication Protocols

- Citibank SSL Gateway Message Specifications
- ISO8583, Base24, HPDH
- TCP/IP, TCP/IP w/ SSL
- HTTP, HTTPS

3.2 *Minimum System Requirements*

Hardware

- Dual CPU Pentium III 1GHz Class Server or equivalent server
- 512GB RAM or above
- 20GB HDD

Software

- Operating System :- Solaris/ Linux/ Windows (or any OS supporting Sun JVM 1.4)
- Database :- Firebird / Oracle 9i / MS-SQL Server 7.0 / DB2 or any Database Server with JDBC Driver
- Application/Web Server :- Apache Web Server 1.3.22 with Tomcat 3.3/Resin Web Server/ WebLogic / Iplanet / Websphere or any application server that supports JSP 1.2 and Servlet 2.3 and above
- Browser:- Internet Explorer 5.0 and above or equivalent (for Merchant to access merchant administration screen)

3.3 Plug-in Fraud Detection Server (FDS) Supported

3.3.1 The Fraud Management Challenge

The continued rapid growth of online commerce presents merchants with new opportunities for revenue and efficiency. Businesses selling goods via the Web, through a call center, or in other situations where a credit card is not present, increases the challenges in managing fraud. According to Gartner G2, the risk of e-Infinity E-Pay fraud is at least 15 times higher than it is for face-to-face transactions.

Merchants selling online are challenged to efficiently manage the increasing risk of fraud due to :

- Purchasers being virtually anonymous
- Online system vulnerability to technology-assisted fraud
- Merchant's liability for fraud losses
- Ever increasing sophistication of fraud schemes and tools

The cost of fraud goes well beyond the value of merchandise lost. It also includes shipping cost, card associations and merchant bank fees, and administrative costs.

Fraud Detection Server (FDS)

FDS is the most effective solution available to reduce cost of fraud and control the risks of card-not-present financial transaction processing. FDS is tightly integrated with the transaction module to provide "risk scoring" for every transaction based on the fraud parameters that can be easily configured. With FDS in place, merchant is able to manage and control fraud with confidence. FDS is a robust and integrated solution that combines :

- The most comprehensive arsenal of risk management technologies to minimize fraud losses
- Complete control of the order screening process to maximize valid sales and customer satisfaction
- An extensible decision platform that will adapt and grow with the business
- No transaction fees to protect merchant's investment
- Enterprise-class reliability, availability, security and scalability for efficiency and performance.

3.3.2 *Maximize Valid Business and Customer Satisfaction*

FDS provides total business user control over the screening and case review processes. The web-based user interface enables the merchant to easily design, deploy, and update an automated screening process. The scoring parameters can be modified based on the merchant's business nature with minimum IT skills required.

FDS minimizes the risk of the merchant for alleged payments. However, the screening and case review processes are performed without impacting the shopping experience of the legitimate customers.

3.3.3 *Flexibility*

FDS provides a flexible and adaptable platform that enables merchants to react immediately to the ever-changing fraud schemes. Furthermore, FDS' open architecture enables integration to third party fraud screening and identity-validation solution.

3.3.4 *Investment Protection*

FDS' licensing model is based on per CPU instead of per transaction fees. This protects the merchant's investment when the transaction volume grows.

3.3.5 *Efficiency and Performance*

Fraud management is an essential function for merchants that conduct card-not-present transactions. FDS is designed and developed with scalable architecture that ensures the efficiency and performance when the transaction loads increase.

3.3.6 *Risk Management Professional Services*

Optimal risk management results require an in-depth understanding of the risk characteristics of the merchant's business. Besides that, risk management is also an ongoing process of analysis and tuning. OCSB offers a variety of professional risk management services designed to help merchants to achieve maximum results.

3.4 Fraud Detection Server Features

3.4.1 Fraud Scoring

Fraud scoring enables the user to create a series of business specific rules, based on any combination of the transaction, order detail data fields and built-in functions. Fraud scoring consists of sophisticated transaction profiling intelligence that provides "risk scoring" for each transaction.

The fraud parameters are as below :

- Email Verification with correctly formed syntax
- Free Public Email Address Check
- Frequency of Purchase
- Multiple Attempt Indicator
- Duplicate Purchase Check
- IP Locator
- Card and card type matching check
- Velocity Check
- Transaction Footprint Check
- High Risk Shipping Country Check
- High Shipping Cost Check
- High Risk Purchase Hour Check
- And many more

3.4.2 Centralized Blacklisted Pool

Merchant that subscribes to Infinitium E-Pay Centralized Blacklist database enjoys the benefits of additional protection against fraudulent transactions. The subscription of the Centralized Blacklisted database enables the merchant to be alerted if the transaction meets the parameters that have been blacklisted in the database such as blacklisted credit card number, email address, IP address, shipping address etc

Features

- Real-time query and matching to Centralized Blacklist database
- Alert Warning to the merchant for matched parameters
- New submission for information of fraudulent transaction to the Centralized Blacklisted database by our large pool of merchants that conduct e-commerce transactions worldwide.

3.4.3 Fraud Tools

Fraud Tools are tools that enable the merchants to verify the fraudulent transactions.

Features

- Shipping Address Verifier
- Reverse lookup on telephone number
- Domain Verifier
- Freight Forwarder Verifier
- IP Locator matching IP to city/state and country

3.4.4 *Minimum System Requirements*

Hardware

- Pentium III 1GHz and above
- 256 MB RAM or above (recommended 512 MB)
- 20GB HDD

Software

- Operating System :- Solaris/ Linux/ Windows (or any OS supporting Sun JVM 1.4)
- Database :- Firebird / Oracle 9i / MS-SQL Server 7.0 / DB2 or any Database Server with JDBC Driver
- Application/Web Server :- Apache Web Server 1.3.22 with Tomcat 3.3/Resin Web Server/ WebLogic / Iplanet / Websphere or any application server that supports JSP 1.2 and Servlet 2.3 and above
- Browser:- Internet Explorer 5.0 and above or equivalent (for Merchant to access merchant administration screen)