Contents

Audience for This Guide ........................................................................................................... ix
Documentation Accessibility ..................................................................................................... ix
How To Use This Guide .......................................................................................................... x
Other Information Sources .................................................................................................... xi
Do Not Use Database Tools to Modify Oracle Applications Data ........................................... xvi
About Oracle ............................................................................................................................. xvi

1 Understanding iPayment

New in this Document ........................................................................................................... 1-1
Overview of Oracle iPayment ................................................................................................. 1-2
Integration with Other Oracle Applications ........................................................................... 1-3
iPayment Architectural Overview ........................................................................................ 1-4
Understanding Credit Card Transactions .............................................................................. 1-6
Understanding Terminal-Based and Host-Based Merchants ............................................... 1-8
Understanding Gateway-Model and Processor-Model Payment Systems ......................... 1-8
Understanding Purchase Cards .............................................................................................. 1-9
Understanding Bank Account Transfers ............................................................................. 1-13
Understanding Offline and Online Payments ...................................................................... 1-14
How the Scheduling System Works ..................................................................................... 1-18
Scheduling Concurrent Programs ......................................................................................... 1-19
Understanding Risk Management ....................................................................................... 1-20
Risk Factors Shipped with iPayment ................................................................................... 1-21
iPayment Routing and Operation ......................................................................................... 1-23
Routing Rule Conditions ..................................................................................................... 1-25
Understanding iPayment Security ......................................................................................... 1-26
2 Administering iPayment

Administering iPayment Overview ........................................................................................................ 2-1
iPayment Administration User Interface .................................................................................................. 2-1
Payment System ......................................................................................................................................... 2-2
Creating a New Payment System ........................................................................................................... 2-2
Modifying a Payment System .................................................................................................................. 2-4
Updating a Default Payment System ...................................................................................................... 2-5
Payee ........................................................................................................................................................ 2-5
Creating a New Payee ............................................................................................................................... 2-5
Modifying a Payee ........................................................................................................................................ 2-7
Inactivating a Payee ..................................................................................................................................... 2-8
Updating the Risk Management Status .................................................................................................... 2-8
Risk Factors ................................................................................................................................................ 2-9
Modifying the Risk Score .......................................................................................................................... 2-10
Modifying the Payment Amount Limit Risk Factor .................................................................................. 2-10
Modifying the Payment History Risk Factor .............................................................................................. 2-11
Modifying the Transaction Amount Risk Factor ........................................................................................ 2-11
Modifying the Time of Purchase Risk Factor ............................................................................................ 2-12
Modifying the AVS Codes Risk Factor ....................................................................................................... 2-13
Modifying the Frequency of Purchase Risk Factor ..................................................................................... 2-14
Modifying Oracle Receivables Risk Codes Risk Factor ........................................................................... 2-14
Modifying Oracle Receivables Credit Rating Codes Risk Factor .............................................................. 2-15
Modifying the Risky Instruments Risk Factor ............................................................................................ 2-16
Modifying the Ship to/Bill to Address Risk Factor ..................................................................................... 2-16
Modifying Oracle Receivables Transactional Credit Limit Risk Factor .................................................. 2-16
Modifying Oracle Receivables Overall Credit Limit Risk Factor ............................................................ 2-16
Risk Formula ................................................................................................................................................ 2-16
Creating a Risk Formula .............................................................................................................................. 2-17
Updating a Risk Formula ............................................................................................................................. 2-18
Deleting a Risk Formula ............................................................................................................................... 2-18
Routing Rule ................................................................................................................................................ 2-19
Viewing Routing Rules ............................................................................................................................... 2-19
Creating Routing Rules ............................................................................................................................... 2-20
Modifying Routing Rules ................................................................. 2-21
Deleting Routing Rules ................................................................. 2-22
Managing Operations ................................................................. 2-22
Performing a Payment Authorization ........................................... 2-23
Searching for Transactions ....................................................... 2-26
Matching Transactions .............................................................. 2-27
Performing a Capture Operation ................................................ 2-28
Viewing Transaction Summary .................................................. 2-28
iPayment Properties ................................................................. 2-30
Modifying iPayment Properties ................................................. 2-32

3 Transaction Reporting
Transaction Reporting Overview ................................................. 3-1
iPayment TR User Interface ....................................................... 3-1
Transaction Summary - Daily ...................................................... 3-2
Transaction Summary - Weekly .................................................. 3-3
Transaction Summary - Monthly ............................................... 3-5
Transaction Summary - Transaction Trends ............................... 3-6
Transaction Summary - Processor Trends ................................. 3-7
Transaction Summary - Card Type Trends ................................. 3-7
Transaction Summary - Failure Trends ...................................... 3-7
Payee Summary ................................................................. 3-8
Daily Summary by Payee ......................................................... 3-8
Weekly Summary by Payee ....................................................... 3-10
Monthly Summary by Payee ..................................................... 3-11
Transaction Summary - Transaction Trends ............................... 3-13
Transaction Summary - Processor Trends ................................. 3-13
Transaction Summary - Card Type Trends ................................. 3-14
Transaction Summary - Failure Trends ...................................... 3-14
Part No.  A95477-03

Oracle Corporation welcomes your comments and suggestions on the quality and usefulness of this document. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most?

If you find any errors or have any other suggestions for improvement, please indicate the document title and part number, and the chapter, section, and page number (if available). You can send comments to us via the postal service.

- Electronic mail: globedoc_us@oracle.com
- FAX: (801) 659-7164  Attention: Oracle Applications Global Financials Documentation
- Postal service:
  Oracle Corporation
  Oracle Applications Global Financials Documentation
  500 Oracle Parkway
  Redwood Shores, CA 94065
  USA

If you would like a reply, please give your name, address, telephone number, and (optionally) electronic mail address.

If you have problems with the software, please contact your local Oracle Support Services.
Preface

Audience for This Guide

Welcome to Release 11i of the Oracle iPayment Concepts and Procedures Guide. This guide assumes you have a working knowledge of the following:

- The principles and customary practices of your business area.
- Oracle iPayment
  
  If you have never used Oracle iPayment, Oracle suggests you attend one or more of the Oracle iPayment training classes available through Oracle University.

- The Oracle Applications graphical user interface.
  
  To learn more about the Oracle Applications graphical user interface, read the Oracle Applications User’s Guide.

See Other Information Sources for more information about Oracle Applications product information.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Standards will continue to evolve over time, and Oracle Corporation is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For additional information,
visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

**Accessibility of Code Examples in Documentation**
JAWS, a Windows screen reader, may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, JAWS may not always read a line of text that consists solely of a bracket or brace.

**Accessibility of Links to External Web Sites in Documentation**
This documentation may contain links to Web sites of other companies or organizations that Oracle Corporation does not own or control. Oracle Corporation neither evaluates nor makes any representations regarding the accessibility of these Web sites.

**How To Use This Guide**

This document contains the information you need to understand and use Oracle iPayment.

This manual contains the following two chapters:

- **Chapter 1, “Understanding iPayment”**
  This chapter provides overviews of the application and its components, explanations of key concepts, features, and functions, as well as the application’s relationships to other Oracle or third-party applications.

- **Chapter 2, “Administering iPayment”**
  This chapter provides process-oriented, task-based procedures for using the user interface to set up the application and perform essential business tasks.

- **Chapter 3, “Transaction Reporting”**
  This chapter provides details of the pages provided for viewing the key performance metrics such as transaction summaries, payee summaries, and other critical performance indicators.
Other Information Sources

You can choose from many sources of information, including online documentation, training, and support services, to increase your knowledge and understanding of Oracle iPayment.

If this guide refers you to other Oracle Applications documentation, use only the Release 11i versions of those guides.

Online Documentation
All Oracle Applications documentation is available online (HTML or PDF).

About Document - Refer to the About document for patches that you have installed to learn about new documentation that you can download. The new About document is available on MetaLink.

Related Documentation
Oracle iPayment shares business and setup information with other Oracle Applications products. Therefore, you may want to refer to other product documentation when you set up and use Oracle iPayment.

You can read the documents online by choosing Library from the expandable menu on your HTML help window, by reading from the Oracle Applications Document Library CD included in your media pack, or by using a Web browser with a URL that your system administrator provides.

If you require printed guides, you can purchase them from the Oracle Store at http://oraclestore.oracle.com.

Documents Related to All Products

Oracle Applications User’s Guide
This guide explains how to enter data, query, run reports, and navigate using the graphical user interface (GUI) available with this release of Oracle iPayment (and any other Oracle Applications products). This guide also includes information on setting user profiles, as well as running and reviewing reports and concurrent processes.

You can access this user’s guide online by choosing “Getting Started with Oracle Applications” from any Oracle Applications help file.
Installation and System Administration

Oracle Applications Concepts
This guide provides an introduction to the concepts, features, technology stack, architecture, and terminology for Oracle Applications Release 11i. It provides a useful first book to read before an installation of Oracle Applications. This guide also introduces the concepts behind Applications-wide features such as Business Intelligence (BIS), languages and character sets, and Self-Service Web Applications.

Installing Oracle Applications
This guide provides instructions for managing the installation of Oracle Applications products. In Release 11i, much of the installation process is handled using Oracle Rapid Install, which minimizes the time to install Oracle Applications, the Oracle8 technology stack, and the Oracle8i Server technology stack by automating many of the required steps. This guide contains instructions for using Oracle Rapid Install and lists the tasks you need to perform to finish your installation. You should use this guide in conjunction with individual product user’s guides and implementation guides.

Oracle Applications Supplemental CRM Installation Steps
This guide contains specific steps needed to complete installation of a few of the CRM products. The steps should be done immediately following the tasks given in the Installing Oracle Applications guide.

Upgrading Oracle Applications
Refer to this guide if you are upgrading your Oracle Applications Release 10.7 or Release 11.0 products to Release 11i. This guide describes the upgrade process and lists database and product-specific upgrade tasks. You must be either at Release 10.7 (NCA, SmartClient, or character mode) or Release 11.0, to upgrade to Release 11i. You cannot upgrade to Release 11i directly from releases prior to 10.7.

Maintaining Oracle Applications
Use this guide to help you run the various AD utilities, such as AutoUpgrade, AutoPatch, AD Administration, AD Controller, AD Relink, License Manager, and others. It contains how-to steps, screenshots, and other information that you need to run the AD utilities. This guide also provides information on maintaining the Oracle applications file system and database.
Oracle Applications System Administrator's Guide
This guide provides planning and reference information for the Oracle Applications System Administrator. It contains information on how to define security, customize menus and online help, and manage concurrent processing.

Oracle Alert User's Guide
This guide explains how to define periodic and event alerts to monitor the status of your Oracle Applications data.

Oracle Applications Developer's Guide
This guide contains the coding standards followed by the Oracle Applications development staff. It describes the Oracle Application Object Library components needed to implement the Oracle Applications user interface described in the Oracle Applications User Interface Standards for Forms-Based Products. It also provides information to help you build your custom Oracle Forms Developer 6i forms so that they integrate with Oracle Applications.

Oracle Applications User Interface Standards for Forms-Based Products
This guide contains the user interface (UI) standards followed by the Oracle Applications development staff. It describes the UI for the Oracle Applications products and how to apply this UI to the design of an application built by using Oracle Forms.

Other Implementation Documentation

Multiple Reporting Currencies in Oracle Applications
If you use the Multiple Reporting Currencies feature to record transactions in more than one currency, use this manual before implementing Oracle iPayment. This manual details additional steps and setup considerations for implementing Oracle iPayment with this feature.

Multiple Organizations in Oracle Applications
This guide describes how to set up and use Oracle iPayment with Oracle Applications' Multiple Organization support feature, so you can define and support different organization structures when running a single installation of Oracle iPayment.
Oracle Workflow Guide
This guide explains how to define new workflow business processes as well as 
customize existing Oracle Applications-embedded workflow processes. You also use 
this guide to complete the setup steps necessary for any Oracle Applications 
product that includes workflow-enabled processes.

Oracle Applications Flexfields Guide
This guide provides flexfields planning, setup and reference information for the 
Oracle iPayment implementation team, as well as for users responsible for the 
ongoing maintenance of Oracle Applications product data. This manual also 
provides information on creating custom reports on flexfields data.

Oracle eTechnical Reference Manuals
Each eTechnical Reference Manual (eTRM) contains database diagrams and a 
detailed description of database tables, forms, reports, and programs for a specific 
Oracle Applications product. This information helps you convert data from your 
existing applications, integrate Oracle Applications data with non-Oracle 
applications, and write custom reports for Oracle Applications products. Oracle 
eTRM is available on Metalink

Oracle Manufacturing APIs and Open Interfaces Manual
This manual contains up-to-date information about integrating with other Oracle 
Manufacturing applications and with your other systems. This documentation 
includes APIs and open interfaces found in Oracle Manufacturing.

Oracle Order Management Suite APIs and Open Interfaces Manual
This manual contains up-to-date information about integrating with other Oracle 
Manufacturing applications and with your other systems. This documentation 
includes APIs and open interfaces found in Oracle Order Management Suite.

Oracle Applications Message Reference Manual
This manual describes Oracle Applications messages. This manual is available in 
HTML format on the documentation CD-ROM for Release 11i.

Oracle CRM Application Foundation Implementation Guide
Many CRM products use components from CRM Application Foundation. Use this 
guide to correctly implement CRM Application Foundation.
Other Information Sources
For more information, see the latest versions of the following manuals:

- Oracle iPayment Implementation Guide
- iPayment JavaDoc (Available on Metalink)
- Apache Server Documentation (http://www.apache.com)
- Oracle iStore and Oracle iMarketing Implementation Guide
- Apache’s mod-ssl documentation (http://www.mod-ssl.org/docs).
- Merchant Connection Kit (MCK) Documentation (http://www.cybercash.com/cashregister/download.html)

Training and Support

Training
Oracle offers training courses to help you and your staff master Oracle iPayment and reach full productivity quickly. You have a choice of educational environments. You can attend courses offered by Oracle University at any one of our many Education Centers, you can arrange for our trainers to teach at your facility, or you can use Oracle Learning Network (OLN), Oracle University’s online education utility. In addition, Oracle training professionals can tailor standard courses or develop custom courses to meet your needs. For example, you may want to use your organization’s structure, terminology, and data as examples in a customized training session delivered at your own facility.

Support
From on-site support to central support, our team of experienced professionals provides the help and information you need to keep Oracle iPayment working for you. This team includes your Technical Representative, Account Manager, and Oracle’s large staff of consultants and support specialists with expertise in your business area, managing an Oracle8i server, and your hardware and software environment.

OracleMetaLink
OracleMetaLink is your self-service support connection with web, telephone menu, and e-mail alternatives. Oracle supplies these technologies for your convenience, available 24 hours a day, 7 days a week. With OracleMetaLink, you can obtain
information and advice from technical libraries and forums, download patches, download the latest documentation, look at bug details, and create or update TARs. To use MetaLink, register at (http://metalink.oracle.com).

**Alerts:** You should check OracleMetaLink alerts before you begin to install or upgrade any of your Oracle Applications. Navigate to the Alerts page as follows: Technical Libraries/ERP Applications/Applications Installation and Upgrade/Alerts.

**Self-Service Toolkit:** You may also find information by navigating to the Self-Service Toolkit page as follows: Technical Libraries/ERP Applications/Applications Installation and Upgrade.

---

**Do Not Use Database Tools to Modify Oracle Applications Data**

*Oracle STRONGLY RECOMMENDS that you never use SQL*Plus, Oracle Data Browser, database triggers, or any other tool to modify Oracle Applications data unless otherwise instructed.*

Oracle provides powerful tools you can use to create, store, change, retrieve, and maintain information in an Oracle database. But if you use Oracle tools such as SQL*Plus to modify Oracle Applications data, you risk destroying the integrity of your data and you lose the ability to audit changes to your data.

Because Oracle Applications tables are interrelated, any change you make using Oracle Applications can update many tables at once. But when you modify Oracle Applications data using anything other than Oracle Applications, you may change a row in one table without making corresponding changes in related tables. If your tables get out of synchronization with each other, you risk retrieving erroneous information and you risk unpredictable results throughout Oracle Applications.

When you use Oracle Applications to modify your data, Oracle Applications automatically checks that your changes are valid. Oracle Applications also keeps track of who changes information. If you enter information into database tables using database tools, you may store invalid information. You also lose the ability to track who has changed your information because SQL*Plus and other database tools do not keep a record of changes.

---

**About Oracle**

Oracle Corporation develops and markets an integrated line of software products for database management, applications development, decision support, and office automation, as well as Oracle Applications, an integrated suite of more than 160
software modules for financial management, supply chain management, manufacturing, project systems, human resources and customer relationship management.

Oracle products are available for mainframes, minicomputers, personal computers, network computers and personal digital assistants, allowing organizations to integrate different computers, different operating systems, different networks, and even different database management systems, into a single, unified computing and information resource.

Oracle is the world’s leading supplier of software for information management, and the world’s second largest software company. Oracle offers its database, tools, and applications products, along with related consulting, education, and support services, in over 145 countries around the world.
Understanding iPayment

This topic group provides overviews of the application and its components, explanations of key concepts, features, and functions, as well as the application’s relationships to other Oracle or third-party applications.

New in this Document

The following features are available in Oracle iPayment 11i:

**Processor-Model Payment Systems**
Oracle iPayment now supports the processor-model payment system that passes payment requests directly to a payment processor. With this enhancement, Oracle iPayment can be integrated with both gateway-model and processor-model payment systems.

Besides supporting credit card transactions, the processor-model payment systems will also support Electronic Fund Transfer (EFT) transactions. Thus, both the gateway and processor-model payment systems now support EFT transactions.

**Multiple Payment System Identifiers**
iPayment has been enhanced to include multiple payment system identifiers for a payee. Multiple payment system identifiers are required because a payee may maintain multiple accounts at a payment system. Using Oracle iPayment, the payee can now configure multiple payment system identifiers for a payment system and route the transactions to the appropriate account. The payment system identifiers represent the accounts maintained by the payee with the payment system. The payee is known to the payment system using the identifiers. Two payees cannot have the same identifier for one payment system.
Transaction Reporting
iPayment offers an executive Transaction Reporting (TR) portal that displays key performance metrics such as transaction summaries, payee summaries, and other critical performance indicators that roll up across all processors, types of cards, and transaction types. iPayment TR users can view the information summarized on a daily, weekly or monthly basis. iPayment provides a graphical view of the various business trends and how they are changing. This helps executive users to take business decisions in real time. iPayment also provides a concurrent manager-based e-mail notification system that relieves the burden of constantly monitoring critical measures.

Overview of Oracle iPayment
Oracle iPayment provides an integrated electronic payment solution for both EC applications and client-server applications. It provides user-friendly access, and the applications have the control of payment processing.

Oracle iPayment supports three electronic payment methods: credit card, purchase card, and EFT transactions. iPayment also supports payment partners such as Verisign and Paymentech.

iPayment offers easy installation, administration, and extension capabilities. The risk management functionality of iPayment can quantify and identify fraudulent online transactions for both business-to-business and business-to-consumer models.

Key Benefits of iPayment
- Integrates with many payment processing systems. This feature allows businesses to offer several payment options to their customers and thus reduce implementation and maintenance costs.
- Provides rules based payment processing. This feature allows businesses to incorporate their existing business operations, rules, and procedures and lower costs by controlling relationships with payment processing vendors.
- Provides security through support for industry standards such as SSL.
- Integrates with other Oracle applications, such as Oracle iStore via Order Capture and Order Management, Oracle Receivables, and a single, open application programming interface (API) to integrate with any web-based, or client-server application.
Integration with Other Oracle Applications

I provides support for both single and multi site installations of electronic commerce (EC) or client-server applications. iPayment also allows both stand-alone businesses and internet service providers to offer electronic payment processing.

Integration with Other Oracle Applications

iPayment integrates with other Oracle applications to provide payment processing across your enterprise. Various applications send payment transaction requests to iPayment for processing. Without iPayment, each of these applications would need to build integration to back end payment (BEP) systems. iPayment saves integration effort by providing a single source to the Back end payment systems such as Verisign, Paymentech, and country-specific or region-specific payment systems.

Example of a Payment Processing Flow Using iPayment and Other Oracle Applications:

1. **Sales application (for example, iStore or TeleSales):** A customer purchases a product and decides to pay by credit card. The sales application submits the order.

2. **Order Capture or Order Management:** Order Capture and Order Management process the order. They use iPayment to verify if the credit card number is valid and authorize the order amount. They can also perform some risk evaluation as part of the authorization.

3. **Oracle Receivables:** When the order is shipped, the credit card information is passed to Oracle Receivables and the billing and credit capture takes place.

4. **Oracle Collections:** When the payment is overdue and your call center begins outbound collection attempts, Oracle Collections uses iPayment to authorize and capture credit card transactions.
iPayment Architectural Overview

iPayment can be integrated with any EC or other sales applications. The integrated iPayment component can communicate with the Oracle database and other servlets to provide payment processing.
iPayment APIs

iPayment provides two types of APIs to simplify the integration of existing or new applications with iPayment for payment processing.

- **Electronic Commerce APIs**
  EC applications can use these APIs to integrate their applications with iPayment. The EC application can be a servlet that plugs into any application server, or it can be a stand-alone application that communicates with iPayment via Java APIs or PL/SQL APIs.

- **Payment System APIs**
  Developers can use these APIs to create payment system servlets. These servlets are usually interfaces that link the payment system software to iPayment to facilitate electronic payment processing. iPayment provides Gateway APIs to interface with payment gateways and XML Processor APIs to interface with payment processors.
iPayment Engine
The iPayment engine contains functionality for multi-payment method support, routing, risk management, etc. It works easily with the APIs.

iPayment Servlets
iPayment consists of the following servlets:

- ECServlet
  The ECServlet provides an interface to the iPayment engine to process payment related operations such as authorization, capture, and return. This servlet is primarily used for the PL/SQL APIs provided by iPayment.

- Payment system servlets
  iPayment provides a complete payment solution, bundling payment system servlets developed by Oracle and its payment system partners. The payment systems communicate with the payment processors and the acquirers or banks to process payment transactions. iPayment includes payment system servlets for Paymentech, CyberCash, First Data (North) and EFS. Some payment systems, such as Verisign, have built their own iPayment servlets.

- Field-installable servlets
  iPayment supports field-installable servlets. These payment system servlets are not bundled with iPayment. This feature allows a payee to acquire a new, additional, or upgraded payment system servlet and configure it in the same way as the payment system servlets bundled with iPayment.

  The ability to add field-installable servlets provides payment flexibility and allows new releases of iPayment and the payment systems to be independent of each other. It also enables EC applications to customize the payment system for their specific needs and regions.

  Field-installable payment system servlets for iPayment are usually available from Oracle’s payment system partners.

Understanding Credit Card Transactions
iPayment handles credit card, purchase card, and EFT transactions. The following information explains the process flow for a typical credit card transaction.
Traditional Credit Card Transactions

Traditional credit card transaction processing involves a customer, a payee, an acquiring bank or processor, and an issuing bank.

A credit card transaction consists of three phases: authorization, settlement, and reconciliation.

- Authorization
  
The customer purchases goods or services and sends credit card information and payment instructions to the payee or business.
  
The payee accepts the authorization request and sends it to the credit card processor through iPayment and the payment system.
  
The processor matches the information with a database maintained by the card issuer (such as Visa or MasterCard) to determine if the customer has enough available credit to cover the transaction. If so, then the processor reserves the funds and sends back an authorization code.

- Settlement
  
Settling transactions includes capturing authorized transactions, processing voids and returns, and batch administration.
  
The payee issues capture, void, return, credit, and close batch functions to the processor through iPayment and the payment system.
  
The processor settles the payment with the issuing bank and causes the funds to transfer to the acquiring bank.

- Reconciliation
  
Depending on the agreement between the payee and the acquiring bank, the acquiring bank sends daily, weekly, or monthly reports to the payee for reconciliation.
  
The payee cross-checks transaction information in the database with the bank statement for reconciliation.

Voice Authorization

Sometimes credit card processing networks decline transactions with a referral message indicating that the merchant must call the cardholder’s issuing bank to complete the transaction. The payment information in such cases is submitted over the phone. If the transaction is approved, the merchant is provided with an
authorization code for the transaction. To facilitate follow-on transactions through iPayment for this voice authorization (for example, capture or void), iPayment provides voice authorization support.

**Understanding Terminal-Based and Host-Based Merchants**

iPayment supports the following processing models that the financial industry uses for credit card transactions:

- **Terminal-Based Merchant**

  The payee or business determines when to close batches of transactions for clearing and settlement, and is responsible to perform the close batch operations. Therefore, the payee or business has more flexibility.

- **Host-Based Merchant**

  In this model, the processor’s host maintains all the transactions and is usually responsible for close batch operations at a predetermined frequency. The payee or business does not have to perform close batch operations. Corrections, such as returns and voids, are sent as new transactions to the host.

**Why Is this Important?**

The choice of being a terminal-based or host-based merchant is generally determined by the business type, number of transactions per day, and the model supported by the acquiring bank. The processing model you choose affects how you perform the settlement operations. For a terminal-based merchant model, you have to perform close batch operations periodically. Consult your inquiring bank for more information at the time of signing up.

**Understanding Gateway-Model and Processor-Model Payment Systems**

Oracle iPayment supports both gateway-model and processor-model payment systems. A gateway-model is an interface between Oracle iPayment and a gateway. A payment gateway is a separate service and acts as an intermediary between the EC application and all the financial networks involved with the transaction, including the customers’ credit card issuer and your merchant account. It checks for validity, encrypts transaction details, ensures they are sent to the correct destination and then decrypts the responses which are sent back to the EC application via iPayment. A processor-model is an interface that enables Oracle iPayment to pass credit card, purchase card, EFT, and Automated Clearing House (ACH) payment requests directly to a payment processor without going through a gateway.
A processor-based system allows authorizations in real-time and follow-up transactions such as captures and credits offline. Offline transactions must be batched together and sent as a single request to the payment system. Hence, all transactions other than authorizations are, by default, performed offline. Offline transactions are sent to the processor when the next batch close operation is attempted.

A batch close operation can be done manually or automatically. In a manual batch close, a call is made to the iPayment close batch API. The iPayment scheduler performs an automatic batch close. To determine the final statuses of all submitted transactions in a batch close, a follow-up call to the batch query API can be made. The follow-up call may be a manual call to the API, or can be made automatically through the iPayment scheduler. The follow-up call must be made some time after the batch is submitted. The actual period of time depends on the processor and the number of transactions in the batch.

**Understanding Purchase Cards**

Purchase Cards, also known as procurement cards, are a special type of charge card. These cards possess more features, capabilities, and controls than standard consumer credit or charge cards. Purchase cards are issued by an organisation (hereafter referred to as buyer) to its employees. The card is generally used by the employees for purchasing corporate supplies and services. Payments are directly made by the buyer to the merchants.

Central billing to the buyer, to which the cards are issued, is done. The merchant receives payment a few days after submitting a transaction and the buyer pays the issuing bank for the aggregate amount of purchases made in the billing period.

A purchase card transaction can contain level II or level III data. For more information on card data levels, see Purchase Card Data Levels. In a typical business-to-business scenario, level III data is used. Purchase cards provide merchants with a mechanism to eliminate the costly paper process of providing and collecting funds for outstanding invoices.

iPayment supports purchase cards requiring level II and level III data. From iPayment's perspective, purchase cards are similar to credit cards, except that the payment processor gets more information in the case of purchase cards.

iPayment only supports Level III data purchase card transactions sent via Oracle Receivables. For more information, please look up the credit card chapter in the 'Oracle Receivables User Guide'.
Benefits of Purchase Cards

To the Merchant

- Accepting purchase cards is crucial to increasing competitiveness. Businesses use purchase cards to cut costs and streamline labor intensive processes to procure goods and services. Many buyers prefer merchants that accept purchase cards.

- Merchants generally receive better rates with purchase cards than with credit cards.

- Purchase cards provide a cleaner payment collection process for merchants. Merchants have the ability to collect their funds in conjunction with the settlement of their credit card transactions.

To the Buyer

- A reconciliation stream by providing purchase order number and additional information.

- Aggregation of purchases when companies receive one invoice for multiple purchase cards.

- Streamlining the purchase order process. Lower processing costs by simplifying the purchasing process, reducing paperwork, and automating controls on the spending limits.

- Merchants accepting purchase card as a payment method help the buyer by making purchase information available electronically. This may help companies (buyers) comply with tax regulations, reporting requirements, and expense reconciliation.

Purchase Card Data Levels
For a purchase card, three levels of data can be captured and sent by a merchant to the buyer organisation. They are:

Level I:
Level I transaction data consists of only basic data. A standard credit card transaction provides Level I data to the processor. The buyer cannot derive any special benefits from purchase card usage if the merchant passes only Level I data.
**Level II:**
Level II transaction data consists of data such as tax amount and order number in addition to Level I data.

**Level III:**
Level III line item detail provides specific purchase information such as item description, quantity, unit of measure and price. This information is very useful to the buyer to help streamline accounting and business practices and to merge payment data with electronic procurement systems.

---

**Note:** Data in the table is only indicative. The actual fields are processor-dependent.

Table 1–1 lists information on data that is passed by iPayment in each level.

**Table 1–1 Sample of data passed by iPayment**

<table>
<thead>
<tr>
<th>Data</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Number</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Card Holder Name</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Card Expiration Date</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Card Holder Billing Address</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Currency Code</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Tax Amount</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Transaction/Order Number</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Ship from Zip Code</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Destination Zip Code</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Discount Amount</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Freight Amount</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Duty Amount</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Line Item Information</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Processing Purchase Card Transactions

The transaction phases in a purchase card transaction are the same as in a credit card transaction. The phases are: authorization, settlement, and reconciliation. See the Understanding Credit Card Transactions for more information about transaction phases.

iPayment passes additional information to the payment system only during the close batch operation. Authorization and other settlement operations carry the same information for purchase cards as they do for credit cards.

The business flow differs on the buyer’s side and for the payment system, but not for the merchant except for the additional information that is passed. The business flow is as follows:

- Buyer places an order and provides payment information. Payment information is entered in the merchant’s system. The information includes: purchase card account number, card expiration date, amount of purchase, applicable sales tax, and purchase order number.
- Buyer authorizes payment by requesting authorization through the payment system and the network.
- Card issuer verifies that the purchase is within the cardholder’s authorized spending limits. Within seconds, the merchant receives either an approval or a denial of the payment request.
- Merchant may display a receipt summarizing the items purchased, total amount of the sale, and any taxes paid.
- Merchant captures the payment by issuing a capture transaction to its processor.
- Funds are transferred from the issuing bank (customer’s bank) to the acquiring bank (merchant’s bank).
- Issues bank bills and collects payment at the end of a billing cycle. The buyer receives a central invoice from the issuer bank for all company cardholder transactions.
- Buyer sends a consolidated payment to the purchase card issuer.
- Each cardholder also receives a monthly memo statement at the end of the billing cycle to review it for accuracy. This statement may be reconciled and approved by management.
- The buyer’s accounting department allocates valid expenses to appropriate projects, cost centers, general ledger, or purchase order accounts.
Understanding Bank Account Transfers

iPayment supports bank account transfers for both business-to-consumer and business-to-business models. Account transfer functionality facilitates electronic transfer of payment amounts from a customer’s bank account to the payee’s bank account. EC applications can use bank account transfers for Electronic Fund Transfers (EFT) and, in the US, for Automated Clearing House (ACH) transactions. EC applications use iPayment as their interface to payment processors that provide connectivity to appropriate clearing house networks. iPayment integrates with Paymentech and Verisign’s PayNow service to provide this feature.

The number of operations supported for EFT is less than for credit card payments because of the current practices and processes involved in processing account transfers. You cannot receive real time response for bank account transfers due to the current practices in account transfer processing. The only status that can be provided is whether the payment was submitted to the processing network or not. iPayment only supports offline payments for bank account transfers. See Understanding Offline and Online Payments for more information.

Interface with Electronic Commerce Applications

EC applications can use the same API for credit card, purchase card, and bank account payments. iPayment routes the request to the correct Back end payment system.

The operations that are supported for bank account transfers are merged into the same framework of operations that are supported for credit card payments. The following operations are supported for bank account transfers:

- Payment request
- Payment modification
- Payment cancellation
- Payment inquiry
- Payment query transaction status

Note: Certain credit card operations are not supported for bank account transfers.
Understanding Offline and Online Payments

Process Flow of a Bank Account Payment Request
1. The EC application calls the iPayment API to schedule an offline bank account transfer payment request.

2. All bank account transfer payments need some lead time before the settlement date. At the time of an API call, iPayment determines whether the payment request can be settled on the requested date or not, based on the lead time of the payment system.

3. If it can be settled, then iPayment accepts the payment request. Otherwise, based on the API parameters, iPayment either rejects the payment request or accepts the payment request with a different settlement date.

4. A scheduled offline payment request can either be modified or canceled before it is routed to the payment system.

5. Once a request is routed to the payment system, the EC application can neither modify nor cancel the request.

6. The payment system routes the payment to the appropriate network.

7. If the payment processor is a payment gateway, then the EC application can query iPayment to retrieve the status of the payment transaction. iPayment, in turn, queries the payment system. If there is any failure on the payment network or at the payment system site while processing the payment, then the payment system responds with those errors.

8. Finally, iPayment updates its tables with the status of the transaction and then returns to the EC application the status of the payment request.

Understanding Offline and Online Payments

iPayment supports two models of payment processing:

- **Online Payment Processing**
- **Offline Payment Processing**

Online Payment Processing
Online payment processing is the model in which payment processing request is immediately forwarded to the Back end payment processor. The results from the processor are immediately returned to the EC application.
Offline Payment Processing
Offline payment processing is the model in which payment requests are not immediately forwarded to Back end payment processors. When an EC application makes a payment processing request in a scheduled mode, or if the payment is predated, the payment information is saved in the iPayment database and is sent to the payment processor at a later time.

The offline method uses a scheduler, a utility that functions at regular intervals. The scheduler browses the stored requests and sends requests to the Back end payment systems and updates to the EC applications.

States of Offline Bank Account Payment Requests
An offline bank account payment request in iPayment, at any given time, can be in one of the following states:

- **Pending**: After the EC application makes a request and before the scheduler routes the request to the payment system.
- **Scheduled**: After routing to the payment system.
- **Submitted**: Once the payment system submits the request to the banking network, for example, ACH network.
- **Canceled**: When a pending payment is canceled by the EC application.
- **Failed**: Failed due to technical errors.
- **Communication Error**: Failed due to communication errors. Transaction may be retried.
- **Unpaid**: Insufficient funds.

The state of a payment is determined on the status of the payment request. To obtain the status of a payment request, EC applications can call the Query Transaction Status API.

The following diagram shows the state diagram of an offline payment request (For bank accounts only).
**States of Offline Credit Card Payment Requests**

At any given time, an offline credit card request in iPayment, can be in one of the following states:

- **Pending**: After the EC application makes a request and before the scheduler routes the request to the payment system.
- **Canceled**: When a pending payment request is canceled.
- **Failed**: Failed due to technical errors.
- **Unpaid**: Insufficient funds.
- **Communication Error**: Failed due to communication errors. Transaction may be retried.
- **Paid**: Sufficient funds.
Figure 1–4  State Transition Diagram of an Offline Payment Request-Credit Card
How the Scheduling System Works

The iPayment scheduler provides the ability to handle payment transactions that cannot be processed in real-time. Such transactions may be of two kinds - transactions that can be processed some time after they are submitted to iPayment, or transactions where the Back end payment system cannot process requests in real-time. Scheduling is also useful for automating recurrent tasks associated such as batch closes. Batch closes are performed in a processor-model payment system like Paymentech.

The iPayment scheduler can be configured to perform specific tasks with each invocation. The tasks to be performed are specified through task parameters. For more information on the task parameters, see ‘Overview of Payment System APIs’ in the Oracle iPayment Implementation Guide. If no task parameters are given to the iPayment scheduler, then all tasks will be performed.

Note:

- A task is performed only once every time the scheduler is invoked, even if the same task appears multiple times in the list of task parameters.
- Two instances of the scheduler must not be active at the same time, even if they are configured to perform different tasks.

<table>
<thead>
<tr>
<th>Table 1–2 Scheduler Task Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task Parameter Name</strong></td>
</tr>
<tr>
<td><strong>BATCHCLOSE</strong></td>
</tr>
<tr>
<td><strong>BATCHQUERY</strong></td>
</tr>
<tr>
<td><strong>BATCHRETRY</strong></td>
</tr>
</tbody>
</table>
How the Scheduling System Works

Scheduling Concurrent Programs

Use the following steps to schedule concurrent requests:

1. Log on to Self Service Applications. Use users - IBYADMIN or SYSADMIN (you can use any user with Payment Administrator responsibility).

2. Choose the Payment Administrator responsibility.

3. From the Main menu, select View -> Requests to open the Find Requests window.

4. Click **Submit a New Request** to open the Submit a New Request window.

5. Select the Single Request option.

6. In the Name field, select the iPayment Scheduler from the list of values.

7. Specify the list of tasks that the scheduler has to perform.

8. To define a schedule, click **Schedule** to open the Schedule window.

---

**Table 1–2 Scheduler Task Parameters**

<table>
<thead>
<tr>
<th>Task Parameter Name</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BANKACCOUNT</td>
<td>Offline bank account transactions are submitted.</td>
</tr>
<tr>
<td>CREDITCARD</td>
<td>Offline credit card transactions are submitted.</td>
</tr>
<tr>
<td>PURCHASECARD</td>
<td>Offline purchase card transactions are submitted.</td>
</tr>
<tr>
<td>EFTBATCHCLOSE</td>
<td>A batch close will be attempted for all EFT payee accounts with processor-model payment systems (e.g. Paymentech).</td>
</tr>
<tr>
<td>EFTBATCHRETRY</td>
<td>A batch close will be attempted for all EFT processor-model batches that failed because of an error (please see below for error types) with the Back end payment system servlet. Since the Back end payment system may have received and processed the batch the first time, a retry could potentially lead to double-billing. It is recommended that batch retries be done manually after the merchant confirms the loss of the first batch, rather than by the scheduler. The three instances when a EFTBatchRetry could occur are:</td>
</tr>
<tr>
<td></td>
<td>1. A communication error occurs with the servlet or the processor.</td>
</tr>
<tr>
<td></td>
<td>2. The database fails (i.e. DB shutdown) while the scheduler is running.</td>
</tr>
<tr>
<td></td>
<td>3. If the number of batches per day has exceeded the limit on that processor.</td>
</tr>
</tbody>
</table>
Defining a schedule can be as simple as submitting as soon as possible or using a more complex schedule.

9. Click **Submit** on the Submit Request window if you want to submit the concurrent request for processing.

**Understanding Risk Management**

Card transactions continue to grow in number, taking an ever-larger share of the payment system and leading to a higher rate of stolen account numbers and subsequent losses by banks and merchants. Improved fraud detection thus has become essential to maintain the viability of the payment system and merchants.

Banks have used early fraud warning systems for some years. iPayment provides similar risk management functionality for credit card and purchase card transactions for EC applications. Risk management functionality is provided for both business-to-business and business-to-consumer models. iPayment includes a number of built-in risk factors and provides the option to the payees to run or not run the risk evaluation functionality for each payment operation. Payees can also run the risk evaluation for operations that handle amounts exceeding a specified amount.

A risk factor includes any information which a payee wants to use to evaluate the risk of a customer wanting to buy goods or services from the payee. Examples of risk factors are: address verification, time of purchase and payment amount. These risk factors can be configured for each payee (merchant or biller).

Risk management functionality enables payees and EC service providers to manage the risk involved in processing transactions online. It allows businesses to have any number of predefined risk factors to verify the identity of their customers, assess their customer credit rating, and risk rating in a secure environment.

Payees can associate the risk factors with different weights as a formula and define any number of risk formulas in iPayment based on their business model. When a Payment Request API is called, the EC application can specify which formula to be used to verify the identity of their customers, assess their customer credit rating, and risk rating in a secure environment. When the EC application calls the Payment Request API with the risk formula specified, iPayment will evaluate the risk and in parallel send the authorization request to the payment system. After getting a response from the payment system, iPayment will return both the authorization code and the risk score to the EC application. The EC application has to now decide whether to continue with the sales process and make a payment capture or discontinue the transaction.
Alternatively, Risk API can be called independent of the Payment Request APIs. Using the Risk API separately allows merchants to evaluate risk first. Depending on the risk score, merchants may not want to send the payment request for authorization. This avoids the overhead of sending an authorization for a potentially risky transaction. Please note that when the EC application calls the Risk API separately, iPayment cannot evaluate the risk scores associated with AVS. iPayment gets the AVS codes directly from the payment system during an authorization request. As no authorization request is send in this scenario, iPayment cannot get AVS codes from the payment system and hence cannot evaluate risks scores associated with AVS.

Risk management helps businesses in reducing manual operational overheads to handle bad transactions and in avoiding costly penalties such as chargebacks from banks.

Risk Factors Shipped with iPayment

The following is a list of basic risk factors shipped with the Risk Management component. These risk factors can be configured per payee.

- **Payment amount limit** is the amount involved in a payment request. It varies from business to business and the risk factor score can be configured for different amount ranges based on the business model.

- **Time of purchase** is the time that a payment request is made by the customer. Site administrators can define the time duration during which the payment requests are high risk and assign the risk factor scores for each duration.

- **Ship to/bill to address** is used to match the ship to address to the bill to address in a payment request. A payment request is considered high risk if these two addresses do not match.

- **Risky payment instruments** are a list of payment instruments (e.g., credit cards, bank accounts) that are considered risky by each payee. These include the instruments that were used by customers earlier and had resulted in fraud or chargebacks. Such a list can be generated internally by the payee or obtained from other sources. If these instruments are reused in a payment request, then the payee may again face fraud or chargeback. Risk management functionality can detect whether risky payment instruments are being used during processing by looking at the risky instrument repository. If the instrument being used for the payment is found in the repository, then the payment is considered a high risk payment. The Risky Instruments Upload Utility adds and deletes a list of risky instruments from the database.
- **Transaction amount** is the total amount of payments made by a customer using the same instrument in a specified duration of time. The duration of time is setup by the user. This is related to the payment amount limit risk factor. A customer can make payments in smaller amounts, which are not captured by the payment amount limit risk factor but can be captured by the transaction amount risk factor. Transaction amount risk factor sums up the total amount of payments in a specific duration of time and captures the risk on that amount. The total number of payments made during a specific time period can be checked by looking at the payment history. The site administrator can set up a time duration and a transaction amount. In evaluating this risk factor, if the total payment amount exceeds the transaction amount within the specified time duration, then the payment is considered a high risk payment.

- **Payment history** tracks the reliability of the payer involved in a payment request. If a payer has a good history of payments over a long duration, then payments requested by this payer are considered to be low risk payments.

- **Address verification service (AVS) check** is the risk involved on the AVS code that is returned by the credit card network. Address verification service is provided by MasterCard and Visa credit card networks to match the billing or shipping address with the address that is maintained for the cardholder by the issuing bank. iPayment does address verification during an authorization request, by calling the payment system with the address and zipcode information along with the payment transaction information. The payment system then does the authorization and also returns various AVS codes to iPayment. Various AVS codes are returned based on the complete address match, zipcode match, street address match, etc. A site administrator can configure all AVS codes returned by the payment systems and their corresponding risk factor scores. This service is only provided in the United States of America.

- **Frequency of purchase** tracks the sudden surge in the use of a payment instrument in a short duration. For a particular payment instrument in a payment request, if the frequency of use in a duration configured is more than the setup value, then the payment request is considered to be a high risk payment.

**Oracle Receivables Risk Factors**

For customers who have both iPayment and Oracle Receivables installed and registered, more risk factors are available. These risk factors are set up in Oracle iPayment and the values of these risk factors are setup in Oracle Receivables.
Receivables stores credit management information about customer accounts such as credit rating, risk rating, etc. The following are risk factors used in risk analysis:

- **Credit limit** is an overall credit limit associated with a customer’s account. If a customer has an outstanding balance and the total amount of payment made by the customer exceeds the overall credit limit, then the payment becomes a high risk payment. Overall credit limit varies from business to business. It can be set up as an overall credit limit at the customer or site level through Oracle Receivables.

- **Transaction credit limit** is the credit limit per transaction associated with a customer’s account. When a payment request exceeds the transaction credit limit, it becomes a risky payment. The transaction credit limit varies from business to business. It can be set up at the customer or site level through Oracle Receivables.

- **Credit rating** is the information that enables payees to effectively manage financial terms with their customers. It is useful for online financing or in evaluating purchases of a large amount by a new customer. Credit Rating is a user defined field and the information can be taken from Oracle Receivables. A payee associates risk scores to credit rating. A higher risk score implies that selling goods or services to the customer is risky.

- **Risk code** is a user defined risk assessment field in Oracle Receivables. It is useful for online financing or for evaluating purchases of a large amount for a new customer. The information is available from Oracle Receivables. A payee associates risk scores to all the risk codes. A higher risk score implies that selling goods or services to the customer is risky.

**iPayment Routing and Operation**

iPayment accepts payment transactions from EC applications and routes them to the appropriate Back end payment systems. The customer uses a web browser or a client application to exchange data with a web or server-based EC application. The EC application sends payment requests to iPayment. Finally, iPayment routes the payment requests to the appropriate payment systems.

**What constitutes a routing rule?**

Every routing rule is made up of three components -

- **Basic Rule Information** - This information is used to select and rank all the rules that may be applicable to a payment transaction. The basic rule
information consists of Rule Name, Payee, Payment Instrument Type, Rule Priority and Status.

- **Destination Information** - The destination information specifies the Back end payment system to which the payment transaction should be routed. The destination information consists of Payment System and Payment System Identifier.

- **Routing Rule Conditions** - This specifies the conditions under which a rule becomes applicable to a payment transaction. A rule condition is comprised of a condition name, a criterion for the condition (such as Amount, Currency, Organization ID, Card Type, Card Number and Bank Routing Number), the type of operation related to the criterion and the value of the criterion. Multiple rule conditions can be defined for a routing rule.

**How Routing Works**

Routing of a payment transaction is based on a set of routing rules set up in the iPayment user interface by the iPayment administrator. The routing engine finds the appropriate Payment System in the following sequence:

1. The routing engine retrieves the rules associated with the Payee and Instrument Type specified in the payment request.

2. The routing rule with the highest priority is evaluated first. If the values in the transaction match the conditions specified in the routing rule, the request is routed to the corresponding Payment System using the specified Payment System Identifier.

3. If the values in the request do not match the conditions specified, the routing rule with the next highest priority is evaluated.

4. In case the payment request values do not match any of the conditions specified, the transaction is routed to the default Payment System using the default Payment System Identifier.

Routing rules are prioritized by an administrator. During processing, the rules are evaluated in the order in which they are prioritized.

iPayment supports credit cards, purchase cards and bank account transfers. The payment methods available depend on the payment system that you decide to use.

Payees and businesses can customize how iPayment routes transactions to the payment systems using routing rules based on their business rules and the available payment methods. For example:
- A business sends all electronic payment transactions to a single payment system: Payment System A.
- A business sends all small or micropayment transactions to Payment System A and all credit card transactions to Payment System B.
- A business sends all bank account transfers under $10 to Payment System A, and all other transactions to Payment System B.
- A business sends all transactions using US dollars to Payment System A and all transactions using other currencies to Payment System B.

**Routing Rule Conditions**

Routing rule conditions determine whether the rule is applicable to a payment transaction. A rule can have multiple rule conditions. A rule is applicable to a payment transaction only if the payment transaction can meet all the conditions for the rule. For example, a payee can route all Visa credit card transactions where the Order Amount is greater than 500 US dollars to Payment System C.

Table 1–3 lists the values in the Operation and Value fields for a selected Payment Instrument Type and Criterion.

<table>
<thead>
<tr>
<th>Table 1–3 Table of Criterion Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Payment Instrument Type</strong></td>
</tr>
<tr>
<td>Purchase Card</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Purchase Card Number</td>
</tr>
<tr>
<td>Credit Card</td>
</tr>
</tbody>
</table>
Understanding iPayment Security

The following security features are recommended to guard against unauthorized access to data and iPayment services. In addition, Apache Server provides several types of authentication that you can use to secure servers, listeners, and servlets.

- Firewall protection
- Secure socket layer (SSL)
- Basic authentication for payment systems
- IP address restriction

<table>
<thead>
<tr>
<th>Table 1–3 Table of Criterion Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Payment Instrument</strong></td>
</tr>
<tr>
<td>Card Type</td>
</tr>
<tr>
<td>Currency</td>
</tr>
<tr>
<td>Amount</td>
</tr>
<tr>
<td>Credit Card Number</td>
</tr>
<tr>
<td>Bank Account</td>
</tr>
<tr>
<td>Org ID</td>
</tr>
<tr>
<td>Currency</td>
</tr>
<tr>
<td>Amount</td>
</tr>
</tbody>
</table>

* - Value can take digits, spaces, dashes and wild card character (%). Thus, if value is 4111%, then the routing rule applies to all cards whose card number begin with "4111".
- Data Privacy

**Firewall Protection**
Oracle strongly recommends that you install iPayment and the payment system servlets on a machine inside the Firewall.

Oracle also recommends that you use one of the following two configuration options to further reduce the risk of data being intercepted as it passes between different parts of iPayment:

- Install all the following components on the same machine:
  - iPayment
  - Payment system servlet
  - EC application
- Use Secure Socket Layer (SSL) to connect distributed components

**Secure Socket Layer**
If either iPayment (or its components) or the EC application is installed in a distributed environment, then Oracle recommends configuring SSL between iPayment and the payment system components.

**Basic Authentication for Payment Systems**
For setting up security for basic authentication, you have to perform some tasks both in iPayment administration user interface and in Apache Server administration tool. While configuring iPayment for a particular payment system using the iPayment administration user interface, you have to assign the payment system user name and password in the Payment system configuration screens. You have to assign the same user name and password in the Apache Server that runs the payment system servlet.

For details on setting up basic authentication in Apache Server, refer the Apache Server documentation.

**IP Address Restriction**
In addition to using the merchant user name and password, you can restrict access to iPayment and payment systems through IP address restriction. By using IP address restriction, a feature of the Apache Server, you can specify one or both of the following parameters:
Understanding Extensibility

- The IP addresses of all trusted hosts (machines from which the web server should accept transaction requests for iPayment)
- The IP addresses of some non-trusted hosts (machines from which the web server should refuse transaction requests for iPayment)

If a request is from a machine on the trusted list, iPayment processes the requested transaction. If the request is from a machine on the non-trusted list, Apache Server denies the request and prevents iPayment from processing it.

Through IP address restriction, you can limit access to all operations from non-trusted machines.

For more information about IP address restriction, including how to specify trusted hosts, see Apache Server documentation.

Data Privacy
iPayment provides data privacy. Sensitive data such as user names, passwords, credit card, purchase card and bank account numbers are encrypted in the database.

Other Security Related Information
- EC applications can be built to use iPayment’s Java APIs. Since this approach avoids the EC App servlet, it prevents the network transfer of sensitive information between EC applications and iPayment.
- Separate HTTP ports for site administration and iPayment administration increases security.
- Security can be increased by using SSL for communication between iPayment and the payment system servlet.

Understanding Extensibility
For extensibility to work, the customer has to implement the oracle.apps.iby.extend.TxnCustomizer interface. This interface has two methods: one method is called immediately before a request is sent to the Back end payment system, and the other method is called immediately after the Back end payment system sends a response. Each method is passed a three letter suffix identifying the Back end payment system, a table of name-value pairs comprising the transaction request/response, and an open database connection so that the custom parameters may be fetched/stored.

Extensibility will typically have the following workflow:
1. The EC application integrating with iPayment first writes custom Back end payment system parameters to the database.

2. It then sends a transaction request to iPayment, during which the extensibility class that was implemented queries the custom parameters and adds them to the request.

3. After a Back end payment system response is generated, the extensibility class is again called and custom parameters sent by the Back end payment system into the database are written. These parameters are queried later by the EC application or the extensibility class itself, which can use them for follow-on transactions.
Understanding Extensibility
This topic group provides process-oriented, task-based procedures for using the user interface to set up the application and perform essential business tasks.

Administration Overview

All setup and administrative functions of iPayment are done through the iPayment user interface. You can log in, create, modify, and deactivate payment systems, payees, risk management properties, and routing rules.

iPayment is administered through a browser-based administration user interface that is implemented using Java and Java Server Pages (JSP). Administering iPayment includes using the iPayment user interface to configure iPayment, to add and configure the payment systems, payees, routing rules, and risk management.

Note: Procedure for creating an iPayment administrative user is documented in Oracle iPayment Implementation Guide.

iPayment Administration User Interface

Table 2–1 lists the tab names and the functionality available from the iPayment administration user interface.
Navigating the iPayment Administration User Interface

The iPayment administration user interface includes the administration tabs and the administration workspace.

The administration tabs on the top of the page, remain visible as you navigate through iPayment. The tabs list the administrative tasks that you can perform. When you click a tab, details for the selected task appear in the administration workspace in the lower portion of the page.

Payment System

You can perform the following tasks from the Payment Systems page. This page lists all the registered payment systems and links to each administration site.

- Creating a New Payment System
- Modifying a Payment System
- Updating a Default Payment System

Creating a New Payment System

Use this procedure to create and register a new payment system from the Create Payment System page. The payment system is permanently registered.

Prerequisites

None
Steps
1. Click the Payment System tab.
   
   The Payment Systems page appears.

2. Click Create.
   
   The Create Payment System page appears.

3. Enter payment system details.
   
   Fields marked with blue asterisks are mandatory fields. See Guidelines on Payment System Fields for a description of all fields.

4. Click Create.

Guidelines on Payment System Fields
Table 2–2 lists the payment system fields.

<table>
<thead>
<tr>
<th>Field/Checkbox Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the payment system being added. This name is used in the iPayment generated pages and reports, and should be a popularly known name of the payment system (for example, Verisign and CyberCash).</td>
</tr>
<tr>
<td>Suffix</td>
<td>Three-character suffix for this payment system to use in iPayment API names (for example, cyb for CyberCash). This has to be unique and is stored in lower-case.</td>
</tr>
<tr>
<td>Payment System Type</td>
<td>The payment system type could be payment gateway or payment processor. Click the appropriate radio button See Understanding Gateway-Model and Processor-Model Payment Systems for more details.</td>
</tr>
<tr>
<td>User Name</td>
<td>User name that is to be used for authentication by the payment system when basic authentication is set up on the payment system servlet. The payment system user name contains a maximum of 30 characters. This field is mandatory for credit card and purchase card payment instruments.</td>
</tr>
<tr>
<td>User Password</td>
<td>The password for the payment system user name. This contains a maximum of 12 characters. This field is mandatory for credit card and purchase card payment instruments.</td>
</tr>
</tbody>
</table>
Modifying a Payment System

Use this procedure to modify the values associated with a payment system from the Payment System Details page.

Prerequisites

None

Steps

1. Determine the payment system for which the properties are to be modified.
2. Click the payment system name from the Payment Systems page.
   The Payment System Details page appears.
3. Modify the fields associated with a payment system.
   See Guidelines on Payment System Fields for field details.
4. Click Update.
Updating a Default Payment System

Use this procedure to update the default payment system per instrument type from the Default Payment System page. Any transaction not routed by the routing rules is routed to the default payment system based on its instrument type.

Prerequisites
None

Steps
1. Click the Payment System tab.
2. Click the Default Payment System subtab.
   The Default Payment System page appears.
3. For each payment instrument, select a default payment system from the drop down list available in the Select Payment System column.
4. Click Update.

Payee

The Payees and Risk Management page displays a list of all the registered payees, their status, and their associated risk management links. You can perform the following tasks from the Payees and Risk Management page:
- Creating a New Payee
- Modifying a Payee
- Inactivating a Payee
- Updating the Risk Management Status

Creating a New Payee

Use this procedure to add a new payee from the New Payee page.

Prerequisites
None
**Steps**

1. Open the New Payee page.

2. Click the Payee tab.
   
   The Payees and Risk Management page appears.

3. Click **Create**.
   
   The Create Payee page appears.

4. Add payee details.

5. To add Identifiers for the Payment Systems, click the icon in the appropriate rows.
   
   The Payment System Identifiers page appears.

6. Enter the Identifier(s) and select one as the default Identifier.
   
   While routing a transaction, if none of the rules match the transaction values, the default Payment System Identifier for the default Payment System is used.

7. Click **Add Payment System Identifier** to add more Identifiers.

8. Click **Continue**.
   
   The Create Payee page appears again.

9. Select the payment instrument and enter the merchant category code.
   
   Fields marked with blue asterisks are mandatory fields. See Guidelines on Payee Fields for a description of all the fields.

10. Click **Create**.
   
    A new payee is created.

**Guidelines on Payee Fields**

Table 2–3 describes the payee fields.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payee Name</td>
<td>Payee Name that appears on the pages and reports generated by iPayment. It is unique and case sensitive.</td>
</tr>
</tbody>
</table>
Modifying a Payee

Use this procedure to change a payee’s properties from the Payee Details page.

**Prerequisites**

None

**Steps**

1. Click the Payee tab.

   The Payees and Risk Management page appears.

2. Click the payee name that appears in the Select Payee column.

   The Payee Details page appears.

3. Modify the fields associated with a payee.

---

*Table 2–3 Payee Fields*

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payee Identifier</td>
<td>iPayment uses the Payee Identifier to identify a particular payee. You cannot modify this identifier after saving it. It is unique, case sensitive and must contain alpha numeric and “_”.</td>
</tr>
<tr>
<td>Status</td>
<td>Payee status is either active or inactive. Select active if you want iPayment to process requests for this merchant. Select inactive to suspend payment processing for a merchant while maintaining access to the payee’s configuration file.</td>
</tr>
</tbody>
</table>
| Payment System Identifier   | Identifier by which this payee is uniquely known to a payment system. It is provided by the payment system. Two payees cannot have the same identifier for one particular payment system. This is case sensitive.  
Each payment system can have more than one Payment System Identifier for the same payee. You can specify a default Identifier. |
| Accepted Payment Instruments| Select the appropriate payment instrument that the payee accepts.                                                                                         |
| Merchant Category Code      | The Merchant Category Code contains the Standard Industrial Classification (SIC) code of the merchant involved in the transaction. |
4. To modify Identifiers for a Payment System, click the icon in the appropriate row.
   The Payment System Identifiers page appears.
5. Add or modify the Identifier(s) and select one as the default Identifier.
6. Click Continue.
   The Payee Details page appears again.
7. Modify the Accepted Payment Instrument and Merchant Category Code, if required.
   See Guidelines on Payee Fields for details.
8. Click Update.

Inactivating a Payee

Use this procedure to inactivate a payee from the Payee Details page.

**Prerequisites**

None

**Steps**

1. Click the Payee tab.
   The Payees and Risk Management page appears.
2. Click the payee name which appears in the Select Payee column.
   The Payee Details page appears.
3. Click Inactive in the Status radio button.
4. Click Update.

Updating the Risk Management Status

Use this procedure to update the risk management status of each payee from the Risk Management Status page.

**Prerequisites**

None
**Risk Factors**

**Steps**

1. Click the Payee tab.  
   The Payees and Risk Management page appears.
2. Click the Enabled or Disabled link in the Risk Management Status column.  
   The Risk Management Status page for that payee appears.
3. Click the Enabled or Disabled radio button.
4. Enter an integer value between 0 and 100 in the Cumulative Risk Threshold field.
5. Click **Update**.

**References**

For more information, see Understanding Risk Management.

**Risk Factors**

You can modify the following risk factors and the risk score from the Risk Factors page. All risk factors and the risk score use default values until the values are modified. After being modified, that particular factor or score only affects that particular payee. The other unchanged factors will continue to use the default values.

- Modifying the Risk Score
- Modifying the Payment Amount Limit
- Modifying the Payment History
- Modifying the Transaction Amount
- Modifying the Time of Purchase
- Modifying the AVS Codes
- Modifying the Frequency of Purchase
- Modifying Oracle Receivables Risk Codes
- Modifying Oracle Receivables Credit Rating Codes

For more information, see Understanding Risk Management.
Modifying the Risk Score

Use this procedure to modify the risk score from the Risk Factors page.

**Prerequisites**
None

**Steps**
1. Click the Payee tab.
   The Payees and Risk Management page appears.
2. Click **Modify** in the Risk Factors column associated with the payee whose risk factor is to be configured.
   The Risk Factors page appears.
3. Select the Risk Score from the Risk Factors list.
   The Risk Score Details page appear.
4. Enter an integer value from 0 to 100 in the Risk Value column.
5. Click **Update**.

Modifying the Payment Amount Limit Risk Factor

Payment amount is the amount involved in a payment request. Its scale varies from business to business. Based on the business model, each risk level varies with different amount ranges. Use this procedure to modify the payment amount limit risk factor from the Risk Factors page.

**Prerequisites**
None

**Steps**
1. Click the Payee tab.
   The Payees and Risk Management page appears.
2. Click **Modify** in the Risk Factors column associated with the payee whose risk factor is to be configured.
   The Risk Factors page appears.
3. Select payment amount limit from the Risk Factor drop-down list.
Modifying the Payment History Risk Factor

This risk factor tracks the reliability of the payer involved in a payment request. If a payer has a good history of payments over a long duration, then payments requested by this payer are considered to be low risk payments. Use this procedure to modify the payment history risk factor by configuring the frequency values from the Risk Factors page.

**Prerequisites**

None

**Steps**

1. Click the Payee tab.

   The Payees and Risk Management page appears.

2. Click **Modify** in the Risk Factors column associated with the payee whose risk factor is to be configured.

   The Risk Factors page appears.

3. Select the payment history from the Risk Factor list.

   The Payment History details appear.

4. Enter a positive integer for the duration value and select a duration time.

5. For each risk level, enter a positive integer representing the lower bound of the frequency range in Greater than or equal to column.

6. Click **Update**.

Modifying the Transaction Amount Risk Factor

The transaction amount is the total amount of payments made using the same instrument in a specified period of time. If the total payment amount exceeds the transaction amount, the payment is considered highly risky. Use this procedure to modify the transaction amount risk factor from the Risk Factors page.
Risk Factors

**Prerequisites**
None

**Steps**
1. Click the Payee tab.
   
   The Payees and Risk Management page appears.
2. Click **Modify** in the Risk Factors column associated with the payee whose risk factor is to be configured.
   
   The Risk Factors page appears.
3. Select the Transaction Amount from the Risk Factor drop-down list.
   
   The Transaction amount details appear.
4. Enter a positive number in the Amount field, a positive integer in the Duration field and select a duration time unit.
5. Click **Update**.

**Modifying the Time of Purchase Risk Factor**

The time of purchase is the time that a payment request is made by the payee’s customer. A risk level can be associated to every hour of the day. No hour can be associated with more than one risk level. Use this procedure to modify the time of purchase risk factor from the Risk Factors page.

**Prerequisites**
None

**Steps**
1. Click the Payee tab.
   
   The Payees and Risk Management page appears.
2. Click **Modify** in the Risk Factors column associated with the payee whose risk factor is to be configured.
   
   The Risk Factors page appears.
   
   The Time of Purchase details appear.
4. For each time range, select the starting and ending hour and its risk level.

5. Click Update.

**Guidelines**

You can add more time ranges and the risk levels associated with them by entering time ranges and risk levels in the last row of the table. You can also delete time ranges by selecting the corresponding check box in the Remove column. No time ranges should overlap.

**Modifying the AVS Codes Risk Factor**

The Address Verification Service (AVS) codes are returned by the payment systems such as CyberCash and others. AVS codes are provided by MasterCard and Visa credit card networks to match the billing address with the address that is maintained for the cardholder by the issuing bank. These codes can be associated with various risk levels. Use this procedure to modify the AVS codes risk factor from the Risk Factor page.

**Prerequisites**

None

**Steps**

1. Click the Payee tab.
   
   The Payees and Risk Management page appears.

2. Click Modify in the Risk Factors column associated with the payee whose risk factor is to be configured.

   The Risk Factors page appears.

3. Select AVS codes from the Risk Factor list.
   
   The AVS codes details appear.

4. Enter the AVS codes (separated by commas) in the Address Verification Service Codes field, corresponding to each risk level.

5. Click Update.

**Note:** If you remove all existing AVS codes, iPayment restores the default values.
Modifying the Frequency of Purchase Risk Factor

The Frequency of Purchase risk factor is used to track sudden surges in the use of a payment instrument in a payment request. If the frequency of use of an instrument in a duration configured is more than the setup value, then the payment request is considered to be a high risk payment.

Use this procedure to modify the frequency of purchase risk factor from the Risk Factors page.

**Prerequisites**
None

**Steps**
1. Click the Payee tab.
   The Payees and Risk Management page appears.
2. Click Modify in the Risk Factors column associated with the payee whose risk factor is to be configured.
   The Risk Factors page appears.
3. Select a Frequency of Purchase from the Risk factors list.
   The Frequency of Purchase details appear.
4. Enter a positive integer for the maximum frequency of payment in the Duration field. Also enter the duration time period.
5. Click Update.

Modifying Oracle Receivables Risk Codes Risk Factor

Use this procedure to modify Oracle Receivables risk codes risk factor from the Risk Factors page. Risk code is a user defined risk assessment field in Oracle Receivables. It is useful for online financing or for evaluating purchases of a large amount for a new customer. A payee associates risk levels with each risk code.

**Prerequisites**
Install and register Oracle Receivables.
Steps
1. Click the Payee tab.
   The Payees and Risk Management page appears.
2. Click Modify in the Risk Factors column associated with the payee whose risk factor is to be configured.
   The Risk Factors page appears.
3. Select Oracle Receivables Risk Codes from the Risk Factors list.
   The Oracle Receivables Risk Codes details appear.
4. Select risk levels corresponding to Oracle Receivables Risk Codes in each row.
5. Click Update.

Modifying Oracle Receivables Credit Rating Codes Risk Factor

Use this procedure to modify Oracle Receivables Credit Rating Codes risk factor from the Risk Factors page. Credit Rating is the information enabling payees to effectively manage financial terms with their customers. It is useful for online financing or for evaluating purchases of large values for a new customer. A payee associates risk levels to each credit rating.

Prerequisites
Install and register Oracle Receivables.

Steps
1. Click the Payee tab.
   The Payees and Risk Management page appears.
2. Click Modify in the Risk Factors column associated with the payee whose risk factor is to be configured.
   The Risk Factors page appears.
3. Select Oracle Receivables Credit Rating Codes from the Risk Factors list.
   Details appear.
4. Select Risk Levels corresponding to Oracle Receivables Credit Rating Codes in each row.
5. Click Update.
Modifying the Risky Instruments Risk Factor

The Risky Instruments risk factor cannot be configured.

Risky instruments are a list of instruments that are considered risky by each payee. These include the instruments that were used by customers earlier and had resulted in fraud or charge backs. If the instrument being used for payment is found in the repository, the payment is considered a high risk payment.

Modifying the Ship to/Bill to Address Risk Factor

The Ship To/Bill to Address risk factor cannot be configured.

Ship to/bill to address is used to match ship to and bill to addresses in the payment request. If the ship to and bill to addresses do not match, the payment request is considered high risk.

Modifying Oracle Receivables Transactional Credit Limit Risk Factor

The Oracle Receivables Transactional Credit Limit risk factor cannot be configured.

Transaction credit limit is the credit limit per transaction assigned by Oracle Receivables. When a payment request exceeds the transaction credit limit, it becomes a risky payment. It varies from business to business and can be set up at customer or site level through Oracle Receivables.

Modifying Oracle Receivables Overall Credit Limit Risk Factor

The Oracle Receivables Overall Credit Limit risk factor cannot be configured.

Credit limit is an overall credit limit assigned at site level. If a customer has an outstanding balance and the total amount of payment made by the customer exceeds the overall credit limit, the payment becomes a high risk payment. It varies from business to business and can be set up at customer or site level through Oracle Receivables.

Risk Formula

You can perform the following procedures from the Risk Formula page. This page lists all the risk formulas available for a selected payee. Every payee created through the administrative user interface generates an implicit risk formula associated with that payee. The implicit risk formula cannot be deleted. It is
generated with equal weights among the default risk factors. The weights for an implicit risk formula can be changed like weights for any other formula.

- Creating a Risk Formula
- Updating a Risk Formula
- Deleting a Risk Formula

References
For more information, see Understanding Risk Management.

Creating a Risk Formula

Use this procedure to create a risk formula from the Risk Formula page.

Prerequisites
None

Steps
1. Click the Payee tab.
   The Payees and Risk Management page appears.
2. Click Create/Modify available below the Risk Formulas column associated with the payee.
   The Risk Formulas page appears. The Risk Formulas page lists the implicit formula for each payee and other risk formulas of this payee.
3. Click Create.
   A new Risk Formula page appears.
4. Enter a unique name for the new risk formula in the Formula Name field.
5. Enter a positive integer weight in percent for each risk factor.
   The total weight of all risk factors should be equal to 100. If Oracle Receivables is installed on your site, Oracle Receivables risk factors also appear on this page.
6. Click Create.
References
For more information, see Understanding Risk Management.

Updating a Risk Formula
Use this procedure to update a risk formula from the Risk Formula page.

Prerequisites
None

Steps
1. Click the Payee tab.
   The Payees and Risk Management page appears.
2. Click Create/Modify available below the Risk Formulas column associated with the payee.
3. Select the risk formula to be modified. Click the name of the formula.
   The Risk Formula Details page appears listing the risk factors and the weights assigned to each of the risk factors.
4. Enter a positive integer weight in percent for each risk factor.
   The total weight of all risk factors should be equal to 100. If Oracle Receivables is installed on your site, Oracle Receivables risk factors also appear on this page.
5. Click Update.

References
For more information, see Understanding Risk Management.

Deleting a Risk Formula
Use this procedure to delete the risk formula, except the implicit risk formula, from the Risk Formula page.

Prerequisites
None
**Steps**

1. Click the Payee tab.
   
   The Payees and Risk Management page appears.

2. Click Create/Modify available below the Risk Formulas column associated with the payee.
   
   The Risk Formulas page appears. The page lists the implicit risk formula for each payee and other risk formulas for this payee.

3. Check the check box available in the Remove column corresponding to the risk formula which is to be deleted.

4. Click Update.

---

**Routing Rule**

You can perform the following tasks from the Routing Rules page.

- Viewing Routing Rules
- Creating Routing Rules
- Modifying Routing Rules
- Deleting Routing Rules

**References**

For more information, see iPayment Routing and Operation.

**Viewing Routing Rules**

Use this procedure to view routing rules from the Routing Rule page.

**Prerequisites**

None

**Steps**

1. Click the Routing Rule tab.
   
   The Routing Rules page appears.

2. To view routing rules for a specific payee, select the payee from the View Rules for a drop down list.
By default, iPayment displays the routing rules for all payees. See Guidelines on Routing Rule Fields for a description of all the fields.

Guidelines
For more information, see iPayment Routing and Operation.

Creating Routing Rules
Use this procedure to create a routing rule from the Create Routing Rule page.

Prerequisites
None

Steps
1. Click the Routing Rule tab.
   The Routing Rules page appears.
2. Click Create.
   The Create Routing Rule page appears.
3. Enter values in the fields on this page.
   Fields marked with blue asterisks are mandatory. See Guidelines on Routing Rule Fields for a description of all the fields.
4. Click Create.

Guidelines on Routing Rule Fields
Table 2–4 describes the routing rule fields.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Name of the Routing rule. This name must be unique across all routing rules. The name can contain alphanumeric characters, spaces and ‘_’ only.</td>
</tr>
<tr>
<td>Rule Priority</td>
<td>Select the new priority from the drop down list.</td>
</tr>
<tr>
<td>Status</td>
<td>Select the status of the Routing Rule as either Active or Inactive.</td>
</tr>
</tbody>
</table>
Table 2–4  Routing Rule Fields

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Instrument Type</td>
<td>Select the Instrument Type for this particular rule. The Instrument Type drives the values contained in the Criterion field.</td>
</tr>
<tr>
<td>Payee</td>
<td>Select the Payee for the rule from the drop-down list. The Payee is the party that must receive the payment.</td>
</tr>
<tr>
<td>When all enabled conditions below are met route to</td>
<td>Select the payment system to which transactions that satisfy the conditions are routed.</td>
</tr>
<tr>
<td>Payment System Identifier</td>
<td>Select the Payment System Identifier from the drop down list. The payee is uniquely known to a payment system using this Identifier.</td>
</tr>
<tr>
<td>Add Rule Condition</td>
<td>You can add rule conditions by clicking the Add Rule Condition button.</td>
</tr>
</tbody>
</table>

Table 2–5 describes the routing rule condition fields.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>At least one rule condition should be enabled.</td>
</tr>
<tr>
<td>Condition Name</td>
<td>The condition name is an input field.</td>
</tr>
<tr>
<td>Criterion</td>
<td>The Criterion field refers to the API fields available for the selected payment instrument. The Criterion type drives the values contained in the Value field.</td>
</tr>
<tr>
<td></td>
<td>When a criterion is chosen from the drop-down list, the page is refreshed to add appropriate values to the Operation and Value fields.</td>
</tr>
<tr>
<td>Operation</td>
<td>To set a rule condition, select an operation from the list of values.</td>
</tr>
<tr>
<td>Value</td>
<td>The Value field is a parameter that iPayment uses to validate the transaction data element. The Value field could be an input field or a list of values.</td>
</tr>
</tbody>
</table>

Modifying Routing Rules

Use this procedure to modify routing rules from the Routing Rule page.
Managing Operations

**Prerequisites**
None

**Steps**
1. Click the Routing Rule tab.
   The Routing Rule page appears.
2. Click the routing rule name which appears below the Select Rule column.
   The Routing Rule Details page appears with all the routing rule fields. See Guidelines on Routing Rule fields.
3. Modify the fields.
   The following fields cannot be modified - Payment Instrument Type and Payee.
4. Click **Update**.

**Guidelines**
For more information, see iPayment Routing and Operation.

Deleting Routing Rules
Use this procedure to delete routing rules from the Routing Rule page.

**Prerequisites**
None

**Steps**
1. Click the Routing Rule tab.
   The Routing Rules page appears.
2. Select the routing rule to be deleted by checking the corresponding check box in the Remove column.
3. Click **Update**.

Managing Operations
A user interface is provided in iPayment to test authorization and capture operations for online processing of credit cards and purchase cards. The user
Performing a Payment Authorization

Use this procedure to perform a test on payment authorization from the Authorization Details page. This procedure can be used to test if the payment system, payee, risk factors, risk formulas, and routing rules are all setup correctly within iPayment.

**Prerequisites**

1. Set up the Payment System, Payee, and Routing Rules during iPayment installation.
2. Set up the Risk Factors and Risk Formulas, if you are also testing Risk Analysis.

**Steps**

1. Click the Operation tab.
   
   The Authorization Details page appears.

2. Enter the Authorization details and click Next.
Performing a Payment Authorization

The Authorization Summary page appears with the details entered in the Authorization Details page.

3. Click **Submit** if you are satisfied with the information entered.

   See Guidelines on Authorization Details Fields. The Authorization Results page appears with the entire response from the system about the Authorization success or Authorization failure.

4. Click **Done** to complete the Authorization operation.

5. To make changes to the selections made in case of a failed operation, click **Back** to navigate to the first Authorization Details page.

**Guidelines on Authorization Details Fields**

Table 2–6 describes the authorization details fields.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payee</td>
<td>The list contains the payees configured in iPayment. The selected payee would be the one receiving payment from this operation.</td>
</tr>
<tr>
<td>Tangible ID/Order ID</td>
<td>An identifier can be made up of alphanumeric characters and the underscore character (_). The entered value will identify this operation. The identifier must be unique for a given payee.</td>
</tr>
<tr>
<td>Amount</td>
<td>The authorization amount in the format matching the currency code. The amount must be a positive value.</td>
</tr>
<tr>
<td>Currency</td>
<td>The currency used for this operation.</td>
</tr>
<tr>
<td>Payment Instrument Type</td>
<td>Either credit card or purchase card. These are the only two payment instruments supported through the iPayment Operations user interface.</td>
</tr>
<tr>
<td>Retry</td>
<td>Select Yes or No. Select Yes, if iPayment did not return a valid response for a previous attempt of the same transaction.</td>
</tr>
<tr>
<td>Authorization Type</td>
<td>Select an authorization type from the list. The Authorization Only operation performs only the authorization operation. Authcapture operation performs both authorization and capture operations. Check the payee’s setup to decide which authorization type is configured for the payee.</td>
</tr>
</tbody>
</table>
Performing a Payment Authorization

### Table 2–6  Authorization Details Fields

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice Authorization</td>
<td>Select either Yes or No button. Select Yes, if an authorization has already been made by contacting the financial institution directly rather than through iPainment, and only if you have an Authorization Code for that authorization issued by the financial institution.</td>
</tr>
<tr>
<td>Authorization Code</td>
<td>If an authorization has already been made by contacting the financial institution directly, rather than through iPainment, and the financial institution has issued an authorization code for that transaction, enter the authorization code in this field and select Yes for Voice Authorization (see above).</td>
</tr>
<tr>
<td>Purchase Order Number</td>
<td>This field appears on the user interface if the payment instrument is a purchase card. It is a number from the payer for this authorization operation.</td>
</tr>
<tr>
<td>Tax Amount</td>
<td>This field appears on the user interface if the payment instrument is a purchase card. The amount of the authorization that is taxable.</td>
</tr>
<tr>
<td>Ship to Zip Code</td>
<td>This field appears on the user interface if the payment instrument is a purchase card. The zip code of the destination where the physical merchandise would be shipped.</td>
</tr>
<tr>
<td>Ship From Zip Code</td>
<td>This field appears on the user interface if the payment instrument is a purchase card. The zip code of the source from where the physical merchandise is shipped.</td>
</tr>
<tr>
<td>Card Number</td>
<td>The payment instrument card number used for authorization.</td>
</tr>
<tr>
<td>CVV2 Value</td>
<td>The Card Security Code for the credit card. Enter the last three or four digits of the number that is printed at the back of your card. iPainment uses the term CVV2, but it supports Mastercard’s CVC2 and Amex’s CID.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The expiration date corresponding to the card number of the instrument. The date the card expires or can no longer be used.</td>
</tr>
<tr>
<td>Card Holder Name</td>
<td>The name that appears on the card corresponding to the payment instrument.</td>
</tr>
<tr>
<td>Card Type</td>
<td>The card type of the payment instrument. Choose Unknown for the card types not in the list.</td>
</tr>
<tr>
<td>Card Subtype</td>
<td>This field appears on the user interface if the payment instrument is a purchase card. The subtype of the purchase card. Choose Unknown for the card types not in the list.</td>
</tr>
<tr>
<td>Street</td>
<td>The number and street name of the customer’s billing address.</td>
</tr>
</tbody>
</table>
Searching for Transactions

You can search for transactions based on one or more criteria in the Search Transactions page. To narrow the search criteria, you must enter as many search criteria as possible. Enter values in the fields on which you want to perform the search.

You can also perform Capture and Re-Authorization follow-on operations on the Matching Transactions page.

**Steps**

1. Click the Operation tab.
   
   The Authorization Details page appears.

2. Click the Follow-On Operation subtab.

---

**Table 2–6  Authorization Details Fields**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>City</td>
<td>The name of the customer’s city in the billing address.</td>
</tr>
<tr>
<td>State</td>
<td>The short code for the customer’s state in the billing address.</td>
</tr>
<tr>
<td>Zip Code</td>
<td>For customers in the United States, the zip code.</td>
</tr>
<tr>
<td>Country</td>
<td>The name of the customer’s country in the billing address.</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>Select the Yes or No radio button. Select Yes if risk analysis is to be performed on this transaction.</td>
</tr>
<tr>
<td>Risk Formula Name</td>
<td>Select a risk formula from the list. It is a formula used to calculate the risk score. This field is only saved if you select Yes for risk analysis.</td>
</tr>
<tr>
<td>Same Shipping and Billing Address</td>
<td>Select Yes if the customer’s shipping and billing addresses are the same. This field is only saved if you select Yes for risk analysis.</td>
</tr>
<tr>
<td>Time of Purchase</td>
<td>Select a time of the day at which this operation is performed. By default the time of the current system appears in this field. This field is only saved if you select Yes for risk analysis.</td>
</tr>
<tr>
<td>Customer Account Number</td>
<td>The Oracle Receivables account number for the customer. This account number is used to retrieve the Oracle Receivables risk factors. This field is only saved if you select Yes for risk analysis.</td>
</tr>
</tbody>
</table>
The Search Transactions page appears. See Guidelines on Search Transaction Fields.

3. Select a payee from the list of registered payees.
4. Enter any other additional search criteria.
5. Click Go.

The Matching Transactions page appears with the details depending on the search criteria entered.

**Guidelines on Search Transaction Fields**

Table 2–7 describes the Search Transaction Fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payee</td>
<td>The list contains payees configured in iPayment that have received payments during previous operations.</td>
</tr>
<tr>
<td>Tangible ID/Order ID</td>
<td>Identifiers used for previous orders. This field is case sensitive. The % sign can be used as a wildcard.</td>
</tr>
<tr>
<td>Starting Date/Ending Date</td>
<td>Date ranges for dates of operations.</td>
</tr>
<tr>
<td>Transaction Status</td>
<td>Current status of each transaction. You can select more than one value for this field. See transaction status diagram for details.</td>
</tr>
</tbody>
</table>

**Matching Transactions**

After performing a search, the Matching Transactions page displays the summary information for transactions matching the search criteria.

**Prerequisites**

- Complete the initial steps for searching a transaction on the Search Transactions page.

**Steps**

1. Click the hypertext value in the TangibleID/OrderID field for which you want to view the details.

The Transaction Summary page appears with the details.
Performing a Capture Operation

You can perform a Capture operation starting at the Matching Transactions page.

Prerequisites
1. Identify the transaction for which the Capture operation is to be performed.
2. The transaction supports Capture as a Follow-On operation.

Steps
1. Click Capture in the Follow-On operations column on the Matching Transactions page.
   The Capture Details page appears. By default, the Amount field contains the Authorized amount.
2. If you want to perform the capture operation for an amount different from the authorized amount, edit the Amount field and click Submit.
   The Capture Results page appears with the status of the capture operation, the Transaction Date, and the Transaction Type.

   Note: The Amount value should be less than or equal to the Authorized amount.

Viewing Transaction Summary

You can view the entire history of a transaction from the Transaction Summary page.
Steps
1. Click TangibleID/OrderID on the Matching Transactions page to review the Transaction Details.

   The Transaction Summary page appears displaying the transaction details for a transaction.

2. Click Done to return to the Matching Transactions page.

3. For more details on a particular transaction, click the Trxn Type link.

   The Trxn Details page appears with the details.

Guidelines on Transaction Details Fields
Table 2–8 describes the fields in the Transaction Details page.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payee</td>
<td>The identifier of the payee who received payment in the operation.</td>
</tr>
<tr>
<td>Tangible ID/Order ID</td>
<td>The identifier for this operation that corresponds to a particular order.</td>
</tr>
<tr>
<td>Amount</td>
<td>The amount for this authorization amount in the format matching the currency code.</td>
</tr>
<tr>
<td>Currency</td>
<td>The currency used for this operation.</td>
</tr>
<tr>
<td>Authorization Code</td>
<td>The authorization code.</td>
</tr>
<tr>
<td>AVS Code</td>
<td>Address Verification Service Code.</td>
</tr>
<tr>
<td>Transaction Date</td>
<td>The date when the transaction is processed.</td>
</tr>
<tr>
<td>Transaction Type</td>
<td>The type of the transaction.</td>
</tr>
<tr>
<td>Credit card Number/Purchase card Number</td>
<td>The credit card or purchase card number used for making payments. For security, only the first four digits of the card number are shown during the transaction review.</td>
</tr>
<tr>
<td>Card Type</td>
<td>The type of credit card or purchase card.</td>
</tr>
<tr>
<td>Auxiliary Message</td>
<td>Additional message from the processor.</td>
</tr>
<tr>
<td>Reference Code</td>
<td>The retrieval reference number.</td>
</tr>
<tr>
<td>Overall Risk Score</td>
<td>The overall score from risk evaluation.</td>
</tr>
</tbody>
</table>
You can use the Property Manager provided by the Admin Console to set up or modify iPayment properties.

All the properties listed below are mandatory and should not be removed or renamed, however their values can be modified.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Threshold</td>
<td>The value set up by the payee to check against overall risk score.</td>
</tr>
<tr>
<td>Risky Transaction</td>
<td>The value in this field is true or false depending on the transaction, whether it is risky or not.</td>
</tr>
<tr>
<td>Payment System Name</td>
<td>The name of the payment system that processed the transaction.</td>
</tr>
<tr>
<td>Error Location</td>
<td>Error location reported by the payment system. It is only present when an error has occurred on the payment system’s side.</td>
</tr>
<tr>
<td>Payment System Code</td>
<td>Error code reported by the payment system. It is only present when an error has occurred on the payment system’s side.</td>
</tr>
<tr>
<td>Payment System Message</td>
<td>Error message reported by the payment system. It is only present when an error has occurred on the payment system’s side.</td>
</tr>
</tbody>
</table>

Note: There are two more properties on the Admin Console. The properties are service.factories and service.oracle.apps.iby.ecapp.PaymentServiceFactory.desc. Do not modify the values of these properties as these are code specific and are needed by iPayment.

iPaymentURL

This property contains the following URL:

http://machine:port/<jsp>/ecapp?

Replace the machine and port with the names of the actual machine and the actual port where the iPayment ECServlet is installed. Also, make sure that “?” is present at the end of the URL or append “?” at the end.
This information is mandatory if your EC applications use iPayment PL/SQL APIs or if your application is an Oracle 3i client.

**Errorfile**
This property specifies the fully qualified name of the error file generated by iPayment. For example: `<path>/iby-error.log`. Make sure you give the absolute path to your logging directory. The error file contains exceptions and error messages. It is always generated regardless of the debug flag.

**Debugfile**
This property specifies the fully qualified name of the debug file generated by iPayment. For example, `<path>/iby-debug.log`. Make sure you give the absolute path to your logging directory. This debug contains debug messages and error messages. It is generated only when the debug flag is turned on.

**Debug**
This property is either true or false. If it is set up to true, iPayment writes debug messages to the Debugfile. The default value is false.

**Http_Proxy**
This property specifies the proxy-URL. For example, `http://www-proxy.us.oracle.com`.

To set up this property with an empty value, insert a string starting with `<`. For example, `<none>`.

**No_Proxy**
This property specifies the domain name for which no proxy is needed. For example, `us.oracle.com`.

To set up this property with an empty value, insert a string starting with `<`. For example, `<none>`.

**xml_base**
The xml_base property specifies the location of files required by iPayment’s XML framework, such as iPayment DTD files. This property should give the location of the $IBY_TOP/xml directory, where $IBY_TOP is expanded to its fully qualified path name. For example, `/usr/appl_top/iby/11.5.0/xml`
xml_log
Optional property xml_log gives the full-qualified pathname of the debug file where XML messages should be written. This file is similar in purpose to the iPayment debug file, but has been separated from it since XML messages are much larger than single debug statements. If no value is specified for this property, then XML logging is disabled.

Modifying iPayment Properties

Modify the following iPayment properties to ensure that PL/SQL API and error functionality work.

iPaymentURL
This property contains the following URL:

http://machine:port/jsp/ecapp?

Replace the machine and port with the names of the actual machine and the actual port where the iPayment ECServlet is installed. Also, make sure that "?" is present at the end of the URL or append "?" at the end.

This information is mandatory if your EC applications use iPayment PL/SQL API.

Errorfile
This property specifies the fully qualified name of the error file generated by iPayment. For example: <your_log_dir>/iby_error.log. Make sure you give the absolute path to your logging directory. The error file contains exceptions and error messages. It is always generated regardless of the debug flag.
This topic group provides details of the pages provided for viewing the key performance metrics such as transaction summaries, payee summaries, and other critical performance indicators.

Transaction Reporting Overview

All business intelligence information is summarized and displayed through the iPayment Transaction Reporting (TR) user interface. iPayment rolls up the key critical performance indicators across all processors, types of cards and transaction types. TR provides a tabular and graphical view of the various business trends and how they are changing. The TR user interface is browser-based and implemented using Java and Java Server Pages (JSP).

iPayment TR User Interface

Table 3–1 lists the tab names and the functionality available from the iPayment TR user interface.

Note: To create a user with the Transaction Reporting (DBC) role, see ‘Creating an Oracle iPayment User’ in the Oracle iPayment Implementation Guide.

<table>
<thead>
<tr>
<th>Tab Name</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction Summary</td>
<td>Transactions are summarized on a daily, monthly and weekly basis.</td>
</tr>
</tbody>
</table>
Navigating the iPayment TR User Interface

The iPayment TR user interface includes the Transaction Summary tab, the Payee Summary tab, and the Reports region space. The Transaction summary and the Payee summary tabs on the top of the page remain visible as you navigate through iPayment. The side navigation bars list the information that you can view. When you click on a navigation bar, summarized information for the selected bar appears in the report display space in the lower portion of the page.

Transaction Summary - Daily

The Transaction Summary tab opens the Credit Card Daily Business Close page. Table 3–2 describes the graphs and reports displayed in this page.

Table 3–2  Description of graphs and reports in the Credit Card Daily Business Close page

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily Summary</td>
<td>Calculates and displays the number and dollar value of transactions on the current date. This is further broken down as:</td>
</tr>
<tr>
<td></td>
<td>- All Transactions</td>
</tr>
<tr>
<td></td>
<td>- Total Authorization Requests</td>
</tr>
<tr>
<td></td>
<td>- Total Capture/Settlement Requests</td>
</tr>
<tr>
<td></td>
<td>- Total Refunds/Credits</td>
</tr>
<tr>
<td></td>
<td>- Total Authorizations Settled</td>
</tr>
<tr>
<td></td>
<td>- Total Authorizations Outstanding</td>
</tr>
<tr>
<td></td>
<td>- Total Credit Card Transactions</td>
</tr>
<tr>
<td></td>
<td>- Total Purchase Card Transactions</td>
</tr>
<tr>
<td>Hourly Transaction Volume</td>
<td>Displays a bar graph depicting the volume of transactions for each hour on the current day.</td>
</tr>
</tbody>
</table>
### Table 3–2 Description of graphs and reports in the Credit Card Daily Business Close page

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction Summary</td>
<td>Calculates and displays the total number of requests, total succeeded requests, total failed requests, and total pending requests on the current date for the following transaction types:</td>
</tr>
<tr>
<td></td>
<td>• Authorization Requests</td>
</tr>
<tr>
<td></td>
<td>• Capture/Settlement Requests</td>
</tr>
<tr>
<td></td>
<td>• Refunds/Credit Requests</td>
</tr>
<tr>
<td>Transaction Failure Summary</td>
<td>Transactions are sorted based on the number of transactions for each ‘cause of failure’. The report displays the top five causes of failure for Authorization and Settlement requests on the current date. For each cause of failure, it displays the number of failures and the dollar value of the transactions.</td>
</tr>
<tr>
<td>Card Type Summary</td>
<td>Summarizes the transactions by card type for the current date. The summary displays the average transaction dollar amount for credit cards, each credit card type, and purchase cards.</td>
</tr>
<tr>
<td>Processor Summary</td>
<td>Summarizes transactions by processor for the current date.</td>
</tr>
<tr>
<td>Transaction Risk Summary</td>
<td>Summarizes transactions screened for risk for the current date. Provides information such as:</td>
</tr>
<tr>
<td></td>
<td>• total number of transactions screened for risk</td>
</tr>
<tr>
<td></td>
<td>• percentage of transactions screened for risk</td>
</tr>
<tr>
<td></td>
<td>• number of transactions identified as risky</td>
</tr>
<tr>
<td></td>
<td>• percentage of transactions identified as risky</td>
</tr>
</tbody>
</table>

### Transaction Summary - Weekly

The Weekly navigation link on the Side Panel Menu opens the Credit Card Daily Business Close - Weekly Summary page.

Table 3–3 describes the reports displayed in this page.
### Table 3–3 Description of reports in the Credit Card Daily Business Close - Weekly Summary page

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weekly Summary</td>
<td>Calculates and displays the number and dollar value of transactions during the last seven days including the current date. This is further broken down as:</td>
</tr>
<tr>
<td></td>
<td>- All Transactions</td>
</tr>
<tr>
<td></td>
<td>- Total Authorization Requests</td>
</tr>
<tr>
<td></td>
<td>- Total Capture/Settlement Requests</td>
</tr>
<tr>
<td></td>
<td>- Total Refunds/Credits</td>
</tr>
<tr>
<td></td>
<td>- Total Authorizations Outstanding</td>
</tr>
<tr>
<td></td>
<td>- Total Authorizations Settled</td>
</tr>
<tr>
<td></td>
<td>- Total Credit Card Transactions</td>
</tr>
<tr>
<td></td>
<td>- Total Purchase Card Transactions</td>
</tr>
<tr>
<td>Transaction Summary</td>
<td>Calculates and displays the total number of requests, total succeeded requests, total failed requests, and total pending requests for the last seven days including the current date for the following transaction types:</td>
</tr>
<tr>
<td></td>
<td>- Authorization Requests</td>
</tr>
<tr>
<td></td>
<td>- Capture/Settlement Requests</td>
</tr>
<tr>
<td></td>
<td>- Refunds/Credit Requests</td>
</tr>
<tr>
<td>Transaction Failure</td>
<td>Transactions are sorted based on the number of transactions for each 'cause of failure'. The report displays the top five causes of failure for Authorization and Settlement requests for the last seven days including the current date. For each cause of failure, it displays the number of failures and the dollar value of the transactions.</td>
</tr>
<tr>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>Card Type Summary</td>
<td>Summarizes transactions by card type for the last seven days including the current date. Displays the average transaction dollar amount for credit cards, each credit card type, and purchase cards.</td>
</tr>
<tr>
<td>Processor Summary</td>
<td>Summarizes transactions by processor for the last seven days including the current date.</td>
</tr>
</tbody>
</table>
Table 3–3 Description of reports in the Credit Card Daily Business Close - Weekly Summary page

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction Risk Summary</td>
<td>Summarizes transactions screened for risk for the last seven days including the current date. Provides information such as:</td>
</tr>
<tr>
<td></td>
<td>• total number of transactions screened for risk</td>
</tr>
<tr>
<td></td>
<td>• percentage of transactions screened for risk</td>
</tr>
<tr>
<td></td>
<td>• number of transactions identified as risky</td>
</tr>
<tr>
<td></td>
<td>• percent of transactions identified as risky</td>
</tr>
</tbody>
</table>

Transaction Summary - Monthly


Table 3–4 describes the reports displayed in this page.

Table 3–4 Description of reports in the Credit Card Daily Business Close - Monthly Summary page

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monthly Summary</td>
<td>Calculates and displays the number and dollar value for transactions during the current month. This is further broken down as:</td>
</tr>
<tr>
<td></td>
<td>• All Transactions</td>
</tr>
<tr>
<td></td>
<td>• Total Authorization Requests</td>
</tr>
<tr>
<td></td>
<td>• Total Capture/Settlement Requests</td>
</tr>
<tr>
<td></td>
<td>• Total Refunds/Credits</td>
</tr>
<tr>
<td></td>
<td>• Total Authorizations Settled</td>
</tr>
<tr>
<td></td>
<td>• Total Authorizations Outstanding</td>
</tr>
<tr>
<td></td>
<td>• Total Credit Card Transactions</td>
</tr>
<tr>
<td></td>
<td>• Total Purchase Card Transactions</td>
</tr>
</tbody>
</table>
Transaction Summary - Daily

Table 3–4  Description of reports in the Credit Card Daily Business Close - Monthly Summary page

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Transaction Summary | Calculates and displays the total number of requests, total succeeded requests, total failed requests, and total pending requests for the following transaction types for the current month:  
  - Authorization Requests  
  - Capture/Settlement Requests  
  - Refunds/Credit Requests |
| Transaction Failure Summary | Transactions are sorted based on the number of transactions for each ‘cause of failure’. The report displays the top five causes of failure for Authorization and Settlement requests for the current month. For each cause of failure, it displays the number of failures and the dollar value of the transactions. |
| Card Type Summary   | Summarizes transactions by card type for the current month. The summary displays the average transaction dollar amount for credit cards, each credit card type, and purchase cards. |
| Processor Summary   | Summarizes transactions by processor for the current month.                                                                                   |
| Transaction Risk Summary | Summarizes transactions screened for risk for the current month. Provides information such as:  
  - total number of transactions screened for risk  
  - percentage of transactions screened for risk  
  - number of transactions identified as risky  
  - percentage of transactions identified as risky |

Transaction Summary - Transaction Trends

The Trends link on the Side Panel Menu opens the Credit Card Trends - Transaction Trends page.

Table 3–5 describes the graphs displayed in this page.

Table 3–5  Description of graphs displayed in the Credit Card Trends - Transaction Trends page

<table>
<thead>
<tr>
<th>Graph Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Transactions</td>
<td>Plots the trend of the number of transactions for the last 12 months, not including the current month.</td>
</tr>
</tbody>
</table>
Transaction Summary - Processor Trends

The Processor link on the Side Panel Menu opens the Credit Card Trends - Processor Trends page.

Table 3–6 describes the graphs displayed in this page.

<table>
<thead>
<tr>
<th>Graph Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Transactions</td>
<td>Plots the trend of the number of transactions by processor for the last 12 months, not including the current month.</td>
</tr>
<tr>
<td>Total Amount</td>
<td>Plots the trend of transaction amounts by processor for the last 12 months, not including the current month.</td>
</tr>
</tbody>
</table>

Transaction Summary - Card Type Trends

The Card Type link on the Side Panel Menu opens the Credit Card Trends - Card Type Trends page.

Table 3–7 describes the graphs displayed in this page.

<table>
<thead>
<tr>
<th>Graph Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Transactions</td>
<td>Plots the trend of the number of transactions by card type for the last 12 months, not including the current month.</td>
</tr>
<tr>
<td>Total Amount</td>
<td>Plots the trend of transaction amounts by card type for the last 12 months, not including the current month.</td>
</tr>
</tbody>
</table>

Transaction Summary - Failure Trends

The Card Type link on the Side Panel Menu opens the Credit Card Trends - Failure Trends page.

Table 3–8 describes the graphs displayed in this page.
The Payee Summary tab opens the Select a Payee page. The Select a Payee page lists the available active payees. The user has to select a payee from this page before proceeding to view the different reports available through this tab. The selected payee becomes the default payee for the reports displayed in this tab. To change a payee, select another payee from the Select a Payee link.

**Guidelines on Payee Fields**

Table 3–9 describes the payee fields.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payee</td>
<td>Name of the merchant that appears on the pages and reports generated by iPayment. It is unique.</td>
</tr>
<tr>
<td>View Details</td>
<td>Click View Details to open the Credit Card Daily Business Close - Daily Summary by Payee page.</td>
</tr>
</tbody>
</table>

**Daily Summary by Payee**

The Daily link on the Side Panel Menu opens the Credit Card Daily Business Close -Daily Summary by Payee page.

Table 3–10 describes the graphs and reports displayed in this page.
Table 3–10  Description of graphs and reports in the Credit Card Daily Business Close - Daily Summary by Payee page

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily Summary</td>
<td>Calculates and displays the number and dollar value for transactions during the current date for the selected merchant. This is further broken down as:</td>
</tr>
<tr>
<td></td>
<td>■ All Transactions</td>
</tr>
<tr>
<td></td>
<td>■ Total Authorization Requests</td>
</tr>
<tr>
<td></td>
<td>■ Total Capture/Settlement Requests</td>
</tr>
<tr>
<td></td>
<td>■ Total Refunds/Credits</td>
</tr>
<tr>
<td></td>
<td>■ Total Authorizations Settled</td>
</tr>
<tr>
<td></td>
<td>■ Total Authorizations Outstanding</td>
</tr>
<tr>
<td></td>
<td>■ Total Credit Card Transactions</td>
</tr>
<tr>
<td></td>
<td>■ Total Purchase Card Transactions</td>
</tr>
<tr>
<td>Hourly Transaction</td>
<td>Displays the volume of transactions for each hour of the current day for the selected merchant in a bar graph.</td>
</tr>
<tr>
<td>Volume</td>
<td></td>
</tr>
<tr>
<td>Transaction Summary</td>
<td>Calculates and displays the total number of requests, total succeeded requests, total failed requests, and total pending requests for the following transaction types for the current date and for the selected merchant:</td>
</tr>
<tr>
<td></td>
<td>■ Authorization Requests</td>
</tr>
<tr>
<td></td>
<td>■ Capture/Settlement Requests</td>
</tr>
<tr>
<td></td>
<td>■ Refunds/Credit Requests</td>
</tr>
<tr>
<td>Transaction Failure</td>
<td>Transactions by the selected merchant are sorted based on the number of transactions for each 'cause of failure'. The report displays the top five causes of failure for Authorization and Settlement requests for the current date. For each cause of failure, the number of failures and the dollar value of the transactions is displayed.</td>
</tr>
<tr>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>Card Type Summary</td>
<td>Summarizes transactions by card type and selected merchant for the current date. Displays the average transaction dollar amount for credit cards, each credit card type, and purchase cards.</td>
</tr>
<tr>
<td>Processor Summary</td>
<td>Summarizes the transactions by processor and selected merchant for the current date.</td>
</tr>
</tbody>
</table>
Weekly Summary by Payee


Table 3–11 describes the reports displayed in this page.

**Table 3–11  Description of reports on the Credit Card Daily Business Close - Weekly Summary by Payee page**

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weekly Summary</td>
<td>Calculates and displays the number and dollar value for the transactions during the last seven days including the current date for the selected merchant. This is further broken down as:</td>
</tr>
<tr>
<td></td>
<td>- All Transactions</td>
</tr>
<tr>
<td></td>
<td>- Total Authorization Requests</td>
</tr>
<tr>
<td></td>
<td>- Total Capture/Settlement Requests</td>
</tr>
<tr>
<td></td>
<td>- Total Refunds/Credits</td>
</tr>
<tr>
<td></td>
<td>- Total Authorizations Settled</td>
</tr>
<tr>
<td></td>
<td>- Total Authorizations Outstanding</td>
</tr>
<tr>
<td></td>
<td>- Total Credit Card Transactions</td>
</tr>
<tr>
<td></td>
<td>- Total Purchase Card Transactions</td>
</tr>
</tbody>
</table>
Table 3–11 Description of reports on the Credit Card Daily Business Close - Weekly Summary by Payee page

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction Summary</td>
<td>Calculates and displays the total number of requests, total succeeded requests, total failed requests, and total pending requests for the following transaction types during the last seven days including the current date for the selected merchant:</td>
</tr>
<tr>
<td></td>
<td>- Authorization Requests</td>
</tr>
<tr>
<td></td>
<td>- Capture/Settlement Requests</td>
</tr>
<tr>
<td></td>
<td>- Refunds/Credit Requests</td>
</tr>
<tr>
<td>Transaction Failure Summary</td>
<td>Transactions by the selected merchant are sorted based on the number of transactions for each 'cause of failure'. The report displays the top five causes of failure for Authorization and Settlement requests during the last seven days including the current date. For each cause of failure, it displays the number of failures and the dollar value of the transactions.</td>
</tr>
<tr>
<td>Card Type Summary</td>
<td>Summarizes transactions by card type and selected merchant for the last seven days including the current date. Displays the average transaction dollar amount for credit cards, each credit card type, and purchase cards.</td>
</tr>
<tr>
<td>Processor Summary</td>
<td>Summarizes transactions by processor and selected merchant for the last seven days including the current date.</td>
</tr>
<tr>
<td>Transaction Risk Summary</td>
<td>Summarizes transactions screened for risk during the last seven days including the current date for the selected merchant. It provides information such as:</td>
</tr>
<tr>
<td></td>
<td>- total number of transactions screened for risk</td>
</tr>
<tr>
<td></td>
<td>- percentage of transactions screened for risk</td>
</tr>
<tr>
<td></td>
<td>- number of transactions identified as risky</td>
</tr>
<tr>
<td></td>
<td>- percentage of transactions identified as risky</td>
</tr>
</tbody>
</table>

Monthly Summary by Payee


Table 3–12 describes the reports displayed in this page.
Table 3–12 Description of reports displayed in the Credit Card Daily Business Close - Monthly Summary page

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monthly Summary</td>
<td>Calculates and displays the number and dollar value for the transactions during the current month for the selected merchant. This is further broken down as:</td>
</tr>
<tr>
<td></td>
<td>• All Transactions</td>
</tr>
<tr>
<td></td>
<td>• Total Authorization Requests</td>
</tr>
<tr>
<td></td>
<td>• Total Capture/Settlement Requests</td>
</tr>
<tr>
<td></td>
<td>• Total Refunds/Credits</td>
</tr>
<tr>
<td></td>
<td>• Total Authorizations Settled</td>
</tr>
<tr>
<td></td>
<td>• Total Authorizations Outstanding</td>
</tr>
<tr>
<td></td>
<td>• Total Credit Card Transactions</td>
</tr>
<tr>
<td></td>
<td>• Total Purchase Card Transactions</td>
</tr>
<tr>
<td>Transaction Summary</td>
<td>Calculates and displays the total number of requests, total succeeded requests, total failed requests, and total pending requests for the following transaction types during the current month for the selected merchant:</td>
</tr>
<tr>
<td></td>
<td>• Authorization Requests</td>
</tr>
<tr>
<td></td>
<td>• Capture/Settlement Requests</td>
</tr>
<tr>
<td></td>
<td>• Refunds/Credit Requests</td>
</tr>
<tr>
<td>Transaction Failure</td>
<td>Transactions by the selected merchant are sorted based on the number of transactions for each 'cause of failure'. The report displays the top five causes of failure for Authorization and Settlement requests for the current month. For each cause of failure, it displays the number of failures and the dollar value of the transactions.</td>
</tr>
<tr>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>Card Type Summary</td>
<td>Summarizes transactions by the selected merchant and card type for the current month. Displays the average transaction dollar amount for credit cards, each credit card type, and purchase cards.</td>
</tr>
<tr>
<td>Processor Summary</td>
<td>Summarizes transactions by processor and selected merchant for the current month.</td>
</tr>
</tbody>
</table>
**Transaction Summary - Transaction Trends**

The Trends link on the Side Panel Menu opens the Credit Card Trends - Transaction Trends by Payee page.

Table 3–13 describes the graphs displayed in this page.

<table>
<thead>
<tr>
<th>Graph Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Transactions</td>
<td>Plots the trend of the number of transactions by the selected merchant for the last 12 months, not including the current month.</td>
</tr>
<tr>
<td>Total Amount</td>
<td>Plots the trend of transaction amounts by the selected merchant for the last 12 months, not including the current month.</td>
</tr>
</tbody>
</table>

**Transaction Summary - Processor Trends**

The Processor link on the Side Panel Menu opens the Credit Card Trends - Processor Trends by Payee page.

Table 3–14 describes the graphs displayed in this page.
Transaction Summary - Card Type Trends

The Card Type link on the Side Panel Menu opens the Credit Card Trends - Card Type Trends by Payee page.

Table 3–15 describes the graphs displayed in this page.

<table>
<thead>
<tr>
<th>Graph Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Transactions</td>
<td>Plots the trend of the number of transactions by the selected merchant and card type for the last 12 months, not including the current month.</td>
</tr>
<tr>
<td>Total Amount</td>
<td>Plots the trend of transaction amounts by the selected merchant and card type for the last 12 months, not including the current month.</td>
</tr>
</tbody>
</table>

Transaction Summary - Failure Trends

The Card Type link on the Side Panel Menu opens the Credit Card Trends - Failure Trends page.

Table 3–16 describes the graphs displayed in this page.

<table>
<thead>
<tr>
<th>Graph Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Transactions</td>
<td>Plots the trend of the number of failed transactions by the selected merchant for each failure type for the last three years, not including the current year.</td>
</tr>
</tbody>
</table>
### Table 3–16  Description of graphs in the Credit Card Trends - Failure Trends page

<table>
<thead>
<tr>
<th>Graph Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Amount</td>
<td>Plots the trend of the total failed transaction amounts by the selected merchant for each failure type for the last three years, not including the current year.</td>
</tr>
</tbody>
</table>