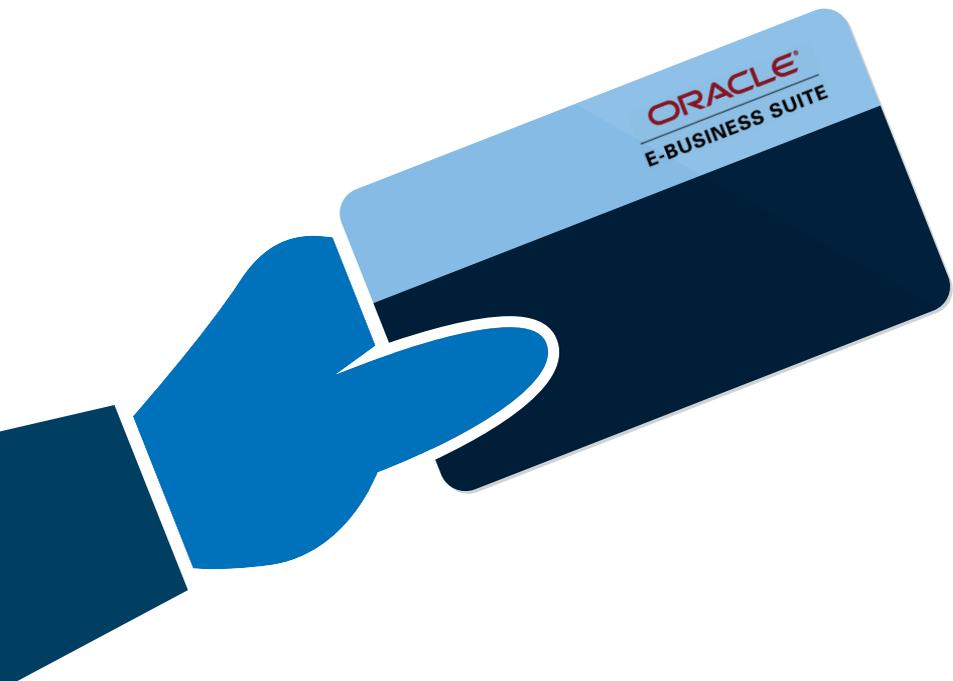


Payments For *Oracle*



What is Payment Processing?

Payments for Oracle is your go-to handbook for understanding payment acceptance technology and security within Oracle E-Business Suite. This document provides a clear and comprehensive understanding on how companies process electronic payments within their ERP as well as guidance on related matters including PCI compliance, the interchange process, EMV technology, and B2B credit card processing.

Table of Contents

1	Types of Payment Solutions
3	Interchange Process
5	Interchange Cost Plus
7	Interchange Cost Plus vs. Tiered Merchant Account Pricing
9	B2B Credit Card Processing
11	Understanding Encryption & Tokenization
12	Standard vs. Integrated Payment Acceptance for Oracle
14	EMV
16	PCI Compliance
18	CardConnect + Oracle E-Business Suite Case Study

Types of Payment Solutions

An Omni-Commerce Solution

For companies accepting payments through Oracle, an integrated, omni-commerce solution is preferred. This allows the Payment Gateway to directly connect to your system without having a separate application to accept payments.

- *Minimizes manual labor associated with payment acceptance*
- *Increases the accuracy of the reconciliation process*

CardConnect's omni-commerce solution for Oracle EBS securely accepts and reconciles payments with a seamless integration.

Business-to-Consumer

Mobile Payments - The umbrella term for accepting credit card transactions from mobile devices. Methods include QR-Code based acceptance, Near Field Communication (NFC), and Card-Present transactions swiped on a piece of hardware (dongle) plugged into a phone.

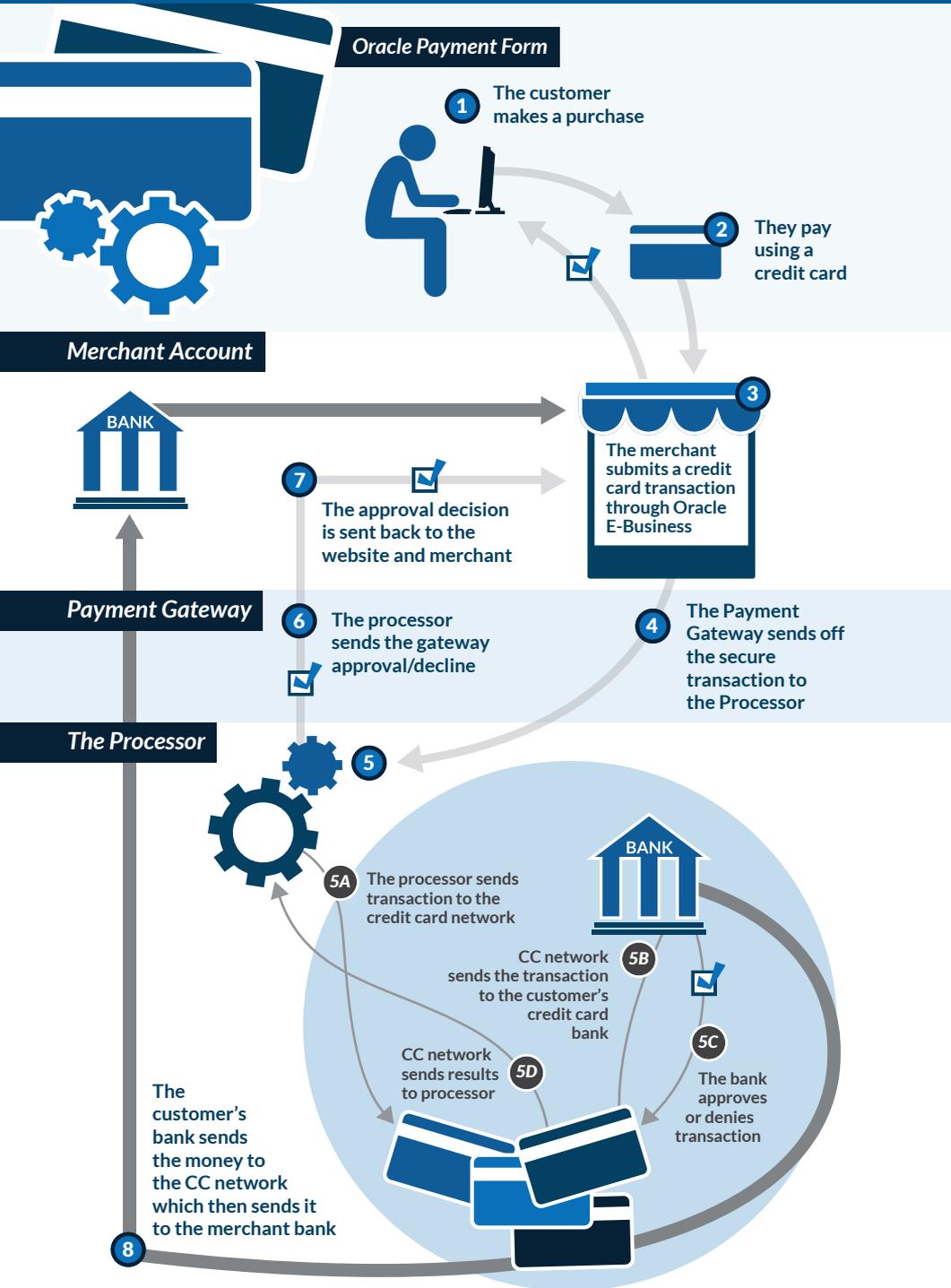
Business-to-Business

Virtual Terminal - A Virtual Terminal is a piece of software or web-based application that allows you to accept transactions from your computer. Virtual Terminals are typically used for card-not-present transactions and are taken over the phone or via mail order.

Payment Gateway - A Payment Gateway is the connector between a payment application (Virtual Terminal, POS System, shopping cart) and the card processing networks. Typically, a Payment Gateway can be "integrated" into these payment applications using an Application Programming Interface (API).



Inside an ERP Transaction



Interchange Process

- 1. The issuing bank in alliance with the cardholder's bank issues a credit card to the cardholder.*
- 2. Cardholder shops at a business that accepts their credit card.*
- 3. Merchant asks buyer for payment for purchase; cardholder presents card.*
- 4. Merchant transmits credit card data and sales amount with an authorization request to their processing company.*
- 5. The processing company routes the transaction to the acquiring bank which processes the transaction, then routes the authorization request to the cardholder's bank. The credit card number identifies the type of card, issuing bank, and the cardholder's account.*
- 6. The acquiring bank which processes the transaction routes the authorization request to the card-issuing bank through the settlement network.*
- 7. The settlement network transmits the data from the cardholder's bank or issuing bank back to the acquiring bank which routes the approval or denial code back to the merchant's Point-of-Sale (POS) terminal or software.*
- 8. The acquiring bank performs what is called an interchange for each sales draft, with the appropriate cardholder's bank. The card-issuing bank transfers the amount of the sales draft, minus an interchange fee to the acquiring bank. The acquiring bank then deposits the amount of all the sales drafts submitted by the merchant, less a discount fee, into the merchant's bank account.*

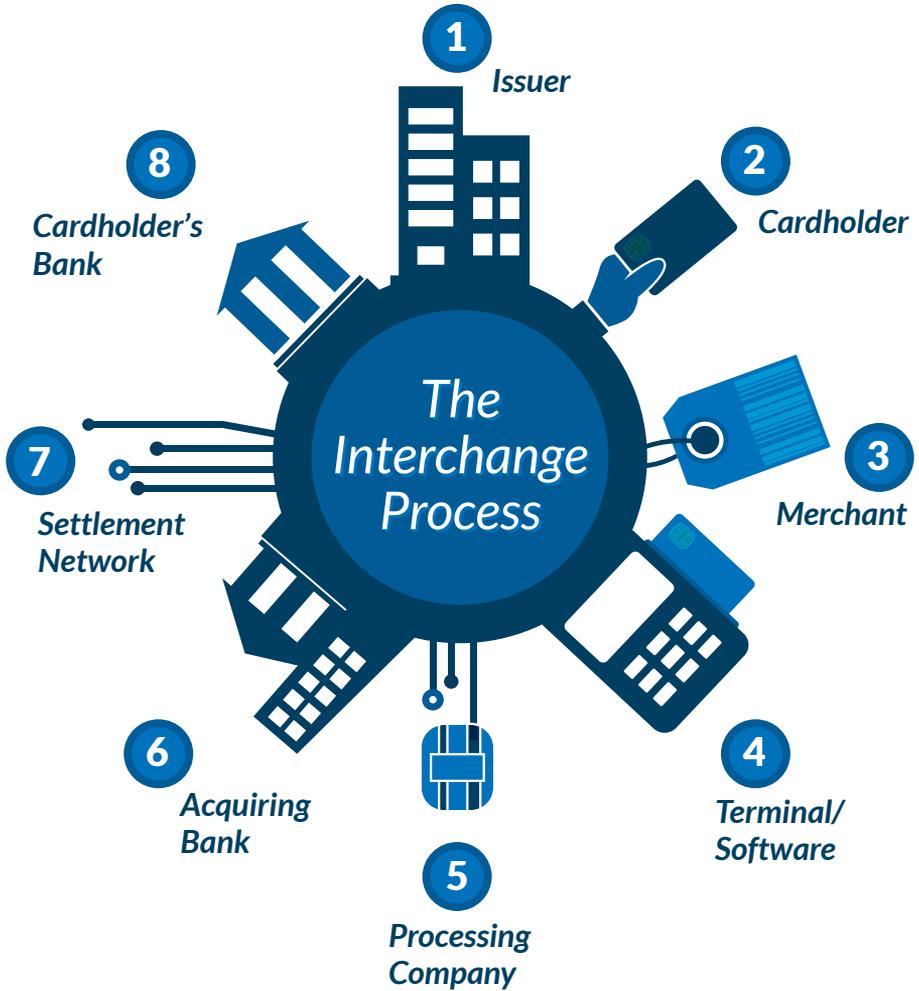
What to know about Interchange

Interchange represents the fees paid to or collected from the card-issuing banks that provide Visa®, MasterCard®, and Discover® cards. These cards may be in the form of Consumer Credit or Debit cards, Corporate, Business, Purchasing cards, and Reward cards.

Visa®, MasterCard®, and Discover® each have their own interchange programs; combined, there are approximately 300 levels of interchange. It is important to know how your business processes transactions and how they are qualifying so you can determine:

- The best interchange level eligibility for your company.*
- How you may reduce your overall processing costs by managing factors which are within your control such as monitoring downgrades, processing Level II and III data, configuring technology properly, transaction timing, operating procedures, and PCI Compliance regulation.*
- Optimal business rules to ensure the highest level of operational efficiency, interchange optimization, and lowest processing costs.*

Interchange Process



Interchange Cost Plus

What is Interchange Cost Plus?

Merchant accounts operating on an interchange cost plus pricing structure may sound more intimidating, but they are actually much more transparent and less expensive than tiered accounts. Certain payment processors offer an interchange cost plus pricing structure, meaning merchants pay the exact interchange fee in addition to a flat markup to their merchant service provider. This eliminates inconsistent buckets and overpaying for inflated tiers.

Unlike tiered accounts that may have several different rate categories, interchange cost plus accounts only have two rates, the interchange markup percentage and a transaction fee.

For example, a business with an interchange cost plus merchant account with a rate of 0.55% and an authorization fee of \$0.15 would pay the wholesale interchange processing rate for every transaction, plus 0.55% and \$0.15 per transaction. The percentage portion of interchange plus pricing is commonly referred to as basis point margin. A basis point is equal to 1/100th of a percent.

Until recently, interchange cost plus pricing was only available to businesses which processed high volumes of credit card sales each month, usually \$35,000 or more. Monthly processing volume and number of transactions ultimately dictates the processor's interchange markup percentage. However, increased competition in the industry has begun to make interchange pricing available to low volume and new businesses.

Questions you should ask about Interchange and your pricing:

- *Does your current processor offer transparency in their billing, or do they intentionally make it hard for you to understand exactly what you are being charged for on each transaction?*
- *What are you really getting from your processor when they debit your account each month for all of their fees? What have they done to help grow your business?*
- *Does your processor care more about charging you a termination fee to keep your business than earning the privilege of serving your needs?*
- *Do you see your current merchant processor as "just another vendor"?*

Interchange Cost Plus

What is Tiered Merchant Account Pricing?

Differential Two-Tier Merchant Account Rate Structure:

- *Qualified Discount Rate (Lowest)*
- *Non-Qualified Discount Rate (Qualified Discount + Differential Interchange Amount + Differential Surcharge = Final Rate)*

Bucketing Three-Tier Merchant Account Rate Structure:

- *Qualified Discount Rate (Lowest)*
- *Mid-Qualified Surcharge (Qualified Discount + Mid-Qualified Surcharge = Final Rate)*
- *Non-Qualified Surcharge (Qualified Discount + Non-Qualified Surcharge = Final Rate)*

Cumulative Three-Tier Merchant Account Rate Structure:

Some processors have additional variations of tiered pricing by adding the cumulative total of downgrades and adding additional transaction fees.

- *Qualified (Lowest)*
- *Mid-Qualified (Qualified + Mid-Qualified Surcharge = Final Rate)*
- *Non-Qualified (Qualified + Mid-Qualified Surcharge + Non-Qualified Surcharge = Final Rate)*

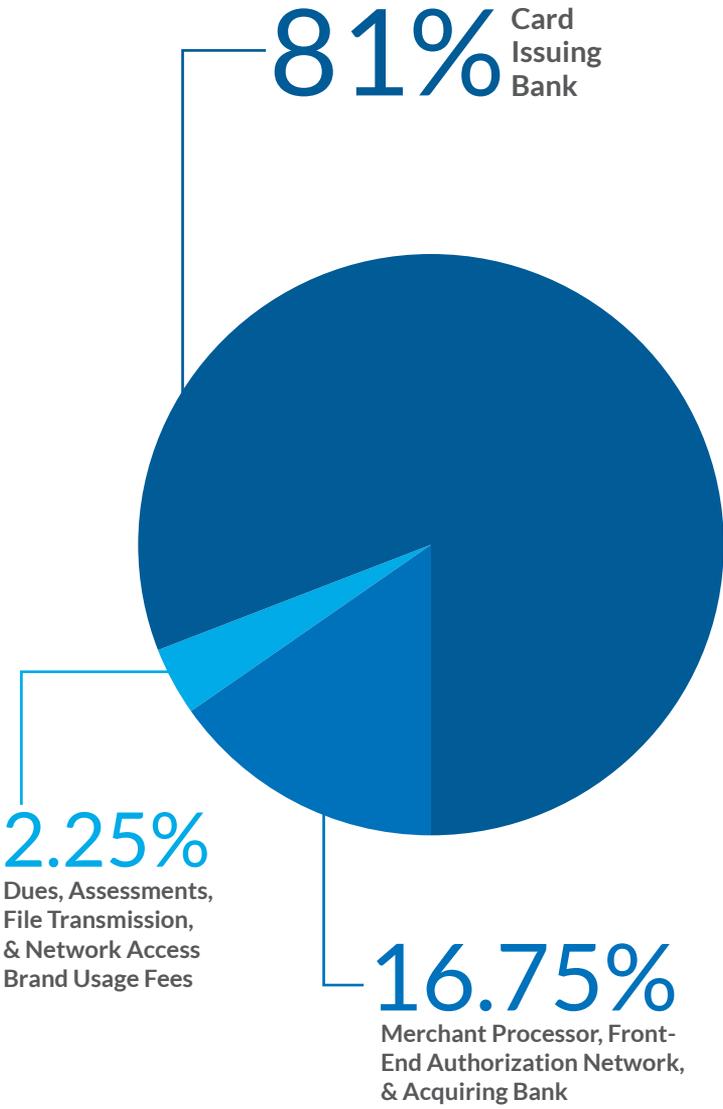
Six-Tier Merchant Account Rate Structure (credit and debit transactions are separated):

- *Qualified Credit Discount Rate (Lowest)*
- *Mid-Qualified Credit Surcharge (Qualified Discount + Mid-Qualified Surcharge = Final Rate)*
- *Non-Qualified Credit Surcharge (Qualified Discount + Non-Qualified Surcharge = Final Rate)*
- *Qualified Debit Discount Rate (Lowest)*
- *Mid-Qualified Debit Surcharge (Qualified Discount + Mid-Qualified Surcharge = Final Rate)*
- *Non-Qualified Debit Surcharge (Qualified discount + Non-Qualified Surcharge = Final rate)*

Interchange Cost Plus vs. Tiered Merchant Account Pricing

<i>Pricing Element</i>	<i>Tiered/ Bucketing</i>	<i>Interchange Cost Plus</i>
Tiered/Bucketing Pricing		
Inconsistent Buckets	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Percentage + Transaction Fee Based on Processor's Formula	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Often Padded April and October with Interchange Adjustments	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Fees Based Upon Gross Sales	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Pass-Through Cost Plus Pricing		
Published Rates on Visa.com and MasterCard.com	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Fixed Rate Above Actual Costs	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Percentage and Transaction Fee + Actual Interchange	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Fees Based Upon Actual Card Type and Qualification	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Manageable Based Upon Card Type	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Fees Based Upon Net Sales	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Cost May Decrease with Interchange Adjustments by Visa®, MasterCard®, and Discover®	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Detailed Card-Level-Billing	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Transparent Easy to Understand	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Lower Overall Cost	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Where do merchant processing fees and interchange costs end up going?*



**Pricing calculations and bucketing strategies vary widely by processor; card type qualifications are for illustration purposes only and do not necessarily represent any specific service provider.*

B2B Credit Card Processing

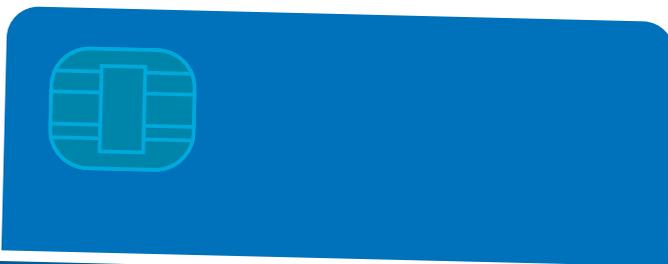
Credit Cards are a common form of payment for Business-to-Business companies. The costs associated with accepting these transactions can be substantial, and it is important to understand certain payment acceptance procedures to ensure your company is qualifying for the lowest rates possible. B2B transactions are more commonly known in the payments industry as “Level 2” and “Level 3” transactions, with Level 2 and Level 3 data referring to the additional data fields that need to be transmitted to the processor to qualify for lower interchange rates.

Level 2 / Level 3 Transactions

Level 2 and Level 3 Transactions are the two different types of Business-to-Business transactions. While Level 2 data includes merchant establishment information and cardholder information, Level 3 data includes line-item detail with product and shipping information. The cards typically utilized for these transactions are business purchasing cards and government cards, for example the GSA SmartPay card.

Interchange Optimization

It is important in a business setting where Level 2 and Level 3 transactions are accepted to proactively manage your interchange costs to ensure you are qualifying the lowest rates possible. For some transactions with a particular type of credit card, the transaction can fall into five different categories (with five different associated fees) based on the information transmitted to the Card Processing Networks. If certain data-points are missing, interchange costs can increase more than 1.00%. There are ways to configure the payment application to require these fields or alternative solutions to ensure your business is qualifying at the lowest rates possible, making it imperative to work with a payments provider that understands these complex transactions.



Transaction Level Requirements

<i>Data Type</i>	<i>Level 1</i>	<i>Level 2</i>	<i>Level 3</i>
<i>Merchant Name</i>	Y	Y	Y
<i>Transaction Amount (Total)</i>	Y	Y	Y
<i>Date</i>	Y	Y	Y
<i>Tax Amount</i>		Y	Y
<i>Customer Code</i>		Y	Y
<i>Merchant Postal Code</i>		Y	Y
<i>Tax Identification</i>		Y	Y
<i>Merchant Minority Code</i>		Y	Y
<i>Merchant State Code</i>		Y	Y
<i>Ship from Postal Code</i>			Y
<i>Destination Postal Code</i>			Y
<i>Invoice Number</i>			Y
<i>Order Number</i>			Y
<i>Item Product Code</i>			Y
<i>Item Commodity Code</i>			Y
<i>Item Description</i>			Y
<i>Item Quantity</i>			Y
<i>Item Unit of Measure</i>			Y
<i>Item Extended Amount</i>			Y
<i>Freight Amount</i>			Y
<i>Duty Amount</i>			Y

Understanding Encryption & Tokenization

Encryption Alone

Encryption involves plain-text data being stored in a way that contains a form of the original text that is unreadable without the appropriate cipher or algorithm. There is a common myth that encrypted data is safe data. In truth, there is no one security method that will protect data completely. Hackers are becoming more and more sophisticated by the day, and while encryption can slow down attacks, it's no match for a skilled cyber-criminal. Encryption is an important and necessary part of the puzzle, but to maximize security it must be combined with tokenization.

Point-to-Point Encryption (P2PE) and Tokenization

When data is protected with a combination of P2PE and tokenization, data is encrypted at the point of interaction, ensuring that the card number is never stored in its original form. That encrypted data is then assigned an identifier known as a token. Tokenized data differs from encrypted data because each token is completely random. This means that there is no pattern that hackers can crack, making the token mathematically irreversible. Sensitive data is then stored in a secure off-site vault.

When credit card numbers are stored in this way, sensitive data never touches a merchant's system, yet is still accessible from the vault for financial reporting.

Reconciliation within Oracle EBS

Processing payments from multiple sources in Oracle E-Business Suite can cause headaches if the right solution isn't in place. Finding an Oracle solution that provides a centralized, transparent environment helps a business manage separate divisions or individual locations simply and efficiently.

This type of solution allows for an easy integration within the Oracle-to-Cash cycle and features the addition of the following functions:

- Collection of all customers' payment data, minimizing penalty fees and collection delays
- Authorization requests to charge the customer's credit
- Automatically compiled list of transactions that have been authorized and delivered

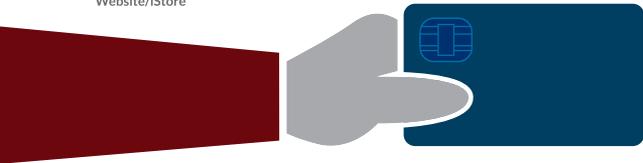
Automate the reporting and reconciliation of your Oracle EBS data, payment gateway, payment processor data, and deposit data within Oracle E-Business without any modifications to your current system.

CardConnect for Oracle EBS efficiently takes an order through the settlement process and sends payment data to domestic and international clearinghouses. Clear receipts from Accounts Receivables, reconcile cash deposits and fees directly within E-Business, and authorize full and partial voids quickly to provide your customers instant reconciliation on returns.

Standard Payment Acceptance for Oracle E-Business Suite



Areas of Concern



Card data stored and transmitted within your environment

Requires PCI questionnaire D and possibly not compliant



Data is only encrypted

Encryption greatly reduces risk, but does not guarantee that information is safe from a hack



No support for level 2 and 3 payment data

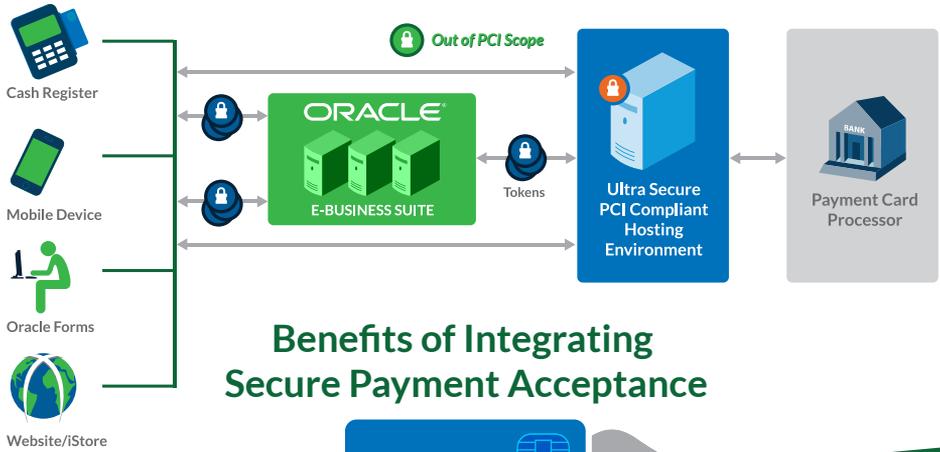
Results in higher interchange fees



Bank deposit information is not reported into Oracle

Creates reconciliation nightmares

Integrated Payment Acceptance for Oracle E-Business Suite



Benefits of Integrating Secure Payment Acceptance



Greatly reduce compliance efforts

Survey decreases from SAQ D to SAQ B for Card-present environments; SAQ D to SAQ A for Card-Not-Present Environments



Reduce costs

Lower interchange rates and encryption costs



Eliminate risk

Maintain brand reputation and customer loyalty; mitigate threats of financial penalties and lawsuits



Increase efficiency

Take advantage of automated bank deposit level reconciliation

Europay[®] Mastercard[®] Visa[®] (EMV)

Chip technology is the latest advancement in the global payments landscape. EMV offers various security features over the traditional magnetic stripe card, preventing card present fraud including card skimming and duplication. A security chip in the card uses cryptography to ensure cardholder verification, validate the card issuer, and verify sensitive data stored on the card. During an EMV transaction, the chip determines the appropriate rules of payment and the terminal enforces these payment rules.

Benefits

- *Global interoperability*
- *Enhanced security*
- *Application processing controls (restrictions or rules can be placed on chip)*
- *Offline data authentication capable*

Incentives for Merchants

A liability shift will take place, transferring accountability for fraud from the card issuer to the merchant or merchant acquirer who has not adopted EMV enabled terminals. With this liability shift, Visa and MasterCard will offer reduced compliance validation requirements which will eventually eliminate the annual mandate of validating PCI DSS compliance.

An upgrade to EMV enabled terminals will prepare merchants with the functionality to accept Radio Frequency Identification (RFID) and Near Field Communications (NFC) mobile payments.

Account Data Compromise (ADC) Relief Waiver for PCI DSS Validation

October 2013, 50% relief if:

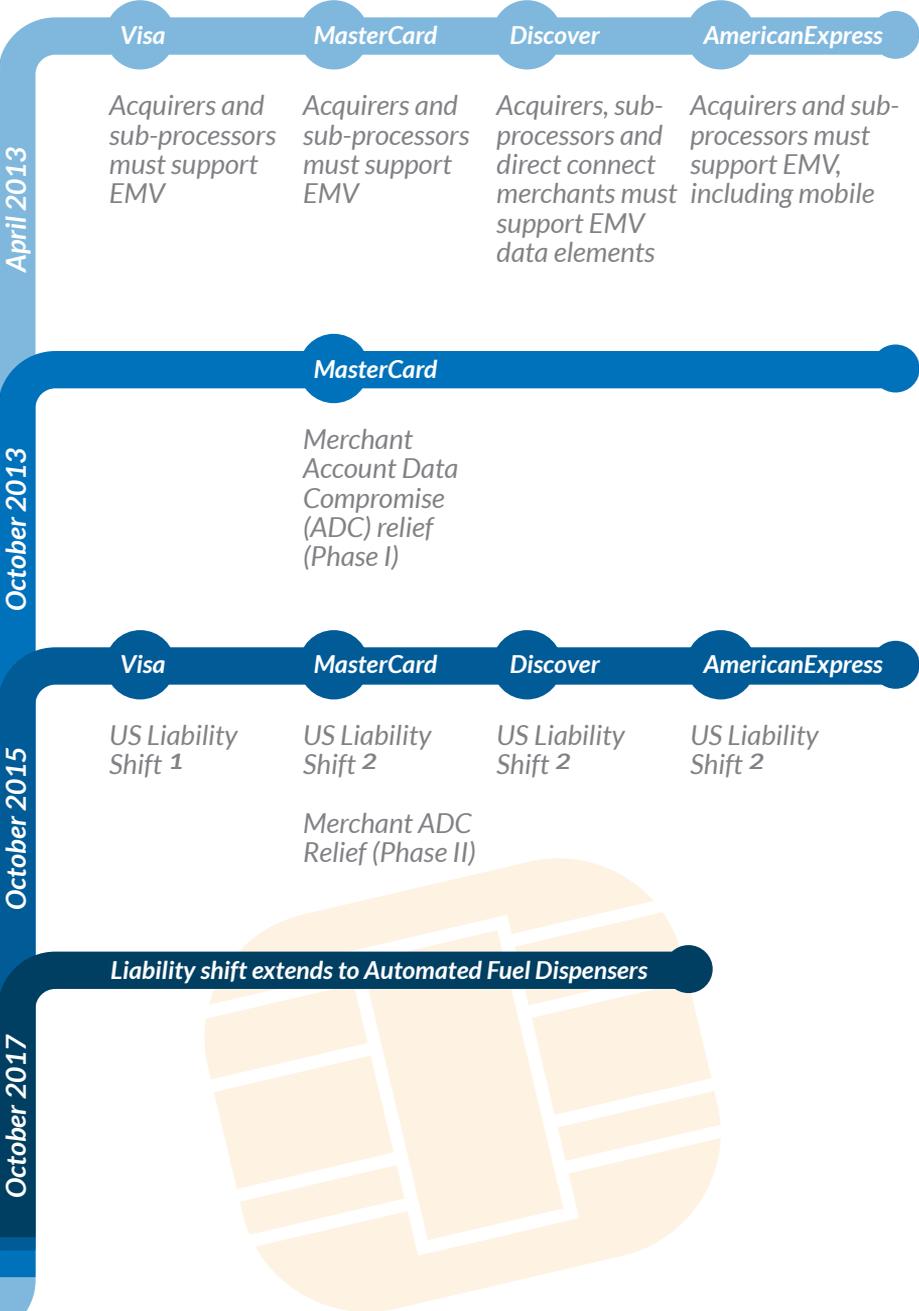
- *75% of transactions processed are initiated at EMV compliant terminals*
- *Merchant has not been involved in a security breach*
- *Merchant must continue to comply with PCI DSS*

Program enrollment required October 2015, 100% relief if:

- *95% of transactions processed are initiated at EMV compliant terminals*
- *Merchant has not been involved in a security breach*
- *Merchant must continue to comply with PCI DSS*
- *Program enrollment required*

EMV Timeline

Visa, MasterCard, Discover & American Express' roadmap to EMV



¹ Liability for counterfeit transaction shifts to party who does not have support for EMV
² Liability for counterfeit transaction shifts to party who has least-secure support for EMV

PCI Compliance

All merchants, whether small or large, need to be PCI compliant. The payment brands have collectively adopted PCI DSS as the requirement for organizations that process, store or transmit payment cardholder data. PCI Security Standards Council™ is responsible for managing the security standards while each individual payment brand is responsible for managing and enforcing compliance to these standards.

Secure Your Business Data

Data Breach: A Very Real Threat

Ensuring the security of electronic payments continues to create new challenges. Criminals are increasingly sophisticated in carrying out network intrusions, wiretapping attacks, and device tampering schemes. Within both the eCommerce and card present spaces, criminals have become more adept at identifying and exploiting security weaknesses to steal valuable cardholder account data and perpetrate fraudulent transactions.

Since early 2005, at least 1.1 billion records of sensitive information have been compromised in publicly announced data breaches.

How data is breached:

- *Hackers who exploit networks and Internet connections without the latest security updates.*
- *Physical losses carried off on flash drives, CDs, DVDs or electronically transferred by dishonest employees.*
- *Third-party thieves who troll trash bins for discarded computers, receipts, and paper records.*

Safeguard Data Entrusted to You

The reality of credit card fraud is not if, but when.

- *You can incur thousands of dollars in costs for audits, forensic investigation, card monitoring, replacement costs, and fines imposed by the card brands.*
- *Your faithful and loyal customers' identity may be compromised.*
- *Small to mid-sized businesses' level of security is easier to target than the large box stores' systems.*
- *The cost of a Level-4 data breach can be \$25,000 to \$50,000, without coverage, a data security breach can easily put you out of business.*



Build Consumer Confidence

The long-term consequences of non-compliance can be disastrous.

- A single incident can severely damage your reputation and hinder your long-term ability to conduct business effectively.
- Account data breaches can lead to catastrophic loss of sales resulting in significant damage to your relationships and good standing in the community.
- Possible negative consequences also include: lawsuits, insurance claims, cancelled accounts, payment card issuer fines, and government fines.

TOP 5 COMPROMISED INDUSTRIES

1

Retail



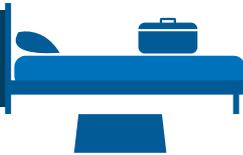
2

Food & Beverage



3

Hospitality



4

Financial Services



5

Nonprofit



CardConnect + Oracle E-Business Suite Case Study

bringing simplified, secure payment acceptance to a decentralized government provider

CardConnect provides Centric Group with a universal payment solution that accommodates the company's various decentralized channels. Not only that, CardConnect integrated the solution seamlessly into Centric's existing Oracle E-Business Suite without modifying the application.

Centric's Situation

Centric Group is a large corporation comprised of a diversified portfolio of companies that provide consumer products to a variety of industries. The decentralized nature of the company had caused a number of operational inefficiencies processing payments. Additionally, as a service provider to the U.S. Department of Justice, Centric required a payment processor with enhanced security to meet a higher level of compliance and security standards.

To address these operational inefficiencies, Centric engaged CardConnect to:

- *Simplify its payment acceptance platform*
- *Integrate payment acceptance directly into its existing Oracle E-Business Suite*
- *Secure its payment processing to meet government compliance and security standards*
- *Remove Centric's Oracle E-Business Suite from PCI Compliance Scope*
- *Standardize its payment processing platform across all portfolio companies*

In Centric's Own Words



"Centric Group is an organization that has always made data security and compliance a high priority. With its CardSecure desktop tokenizer and impressive Oracle integration capabilities, CardConnect was the perfect fit for enhancing the security of our payment processing. On top of that, CardConnect's Interchange Optimization made sure we eliminated unnecessary payment processing costs. As a company that is approaching \$1 billion in yearly revenue, that quantifiable cost-reduction was significant, to say the least."

- Lee R., CIO, Centric Group

CardConnect + Oracle E-Business Suite Case Study

The CardConnect Solution

CardSecure (Desktop Tokenizer) - The desktop tokenizer allowed Centric to tokenize card numbers, then encrypt and store the sensitive data in the CardConnect PCI compliant data center. CardSecure intercepts incoming card data before it hits Oracle E-Business, transfers the data to the secure vault, encrypts it and assigns each card number a unique token. For Centric, this meant that the token, not the sensitive card data, is stored on its system while the actual card data remains securely outside Centric's ERP application.

CardConnect for Oracle - The CardConnect Gateway is an Oracle-Validated integration solution that accelerates cash receipts and provides a direct connection between Oracle EBS and the banking system. With the CardConnect Gateway, Centric's Oracle E-Business system was able to:

- *Efficiently process orders from authorization to settlement*
- *Send payment data to domestic and international clearinghouses*
- *Reconcile cash deposits and fees directly within Oracle E-Business*

CardConnect Interchange Optimization - The CardConnect gateway ensures the lowest possible interchange costs by adding Level II and Level III data for each transaction, along with creating operational procedures to qualify Centric for the lowest interchange rates. Now that these transactions are optimized, Centric is experiencing a quantifiable cost-reduction.

Through this three-step solution, Centric was able to:

- Integrate this payment solution into its ERP quickly and easily
- Process Level II and Level III data to qualify for low Interchange rates
- Remove its Oracle E-Business system from PCI Compliance Scope
- Consolidate omni-channel payment acceptance into Oracle E-Business
- Reconcile cash deposits and fees directly within Oracle E-Business
- **Avoid modifications to its Oracle E-Business system**

CardConnect is an Oracle Validated solution that reduces the cost and risk of credit card processing within Oracle EBS.



