JDEtips
JD Edwards Knowledge. Transferred. Sustained.

December 2013 Distribution/Sales Order Management

PCI Compliance for JD Edwards

By Milind Joshi

Editor's Note: This article explains the common JDE applications where PCI compliance is necessary, helps you understand the processes and risks, then describes two methods for obtaining compliance. The first method describes using JDE along with the associated challenges you will face when choosing this method while the second method outlines an add-on solution and the benefits you will receive if selected. In the end, you will have a solid understanding of the payment processing cycle.

In today's e-cash society, customers in both B2B and B2C space assume that credit cards, Automatic Clearing House (ACH), Electronic Funds Transfer (EFT), e-checks, and other similar features are available for payment processing. Companies that allow this flexibility must be compliant with the rules set by the [i]Payment Card Industry (PCI) Data Security Standards (DSS) Council, and they may be subjected to an annual security assessment conducted by a qualified security assessor as per the standards set by the PCI DSS. Non-compliance can lead to punitive fines and can trigger further liabilities. Because most companies use several applications besides an ERP solution like JD Edwards, PCI compliance assessment can snowball into a complex, time- consuming, and expensive proposition. This white paper recommends an approach that helps companies isolate credit card information from their enterprise applications and significantly limit the breadth of the PCI assessment, and consequently, the encumbrance it imposes on the company.

Introduction

Most companies allow customers to place orders via telephone, email, fax, EDI, and online storefronts. In some cases, sales representatives (SR) also accept orders. Credit card information is typically shared (or accessed) either during the order creation process, when settling open invoices, or while paying for out-of-warranty repairs. Multiple departments such as customer service, service and warranty, accounts receivable and sales, as well as external organizations like payment gateways, payment processors and merchant banks, may be involved in accessing and processing this information. The fact that private credit card information is revealed to numerous people exposes the company to the liability of credit card fraud.

The complexities of the information technology landscape can further compound these risks as organizations acquire and implement diverse software and hardware to support their business processes.

Common Applications are:

- Warehousing, including the use of barcode scanning devices
- Supplier Collaboration
- Manufacturing Execution system
- Product Lifecycle Management
- Customer Relationship Management
- Shipping Optimization

Many business processes transcend the boundaries of individual applications and demand constant information flow and collaboration between various applications. When a piece of critical information is exposed in one application, there is a risk of the exposure cascading over to other applications. This perpetuates the risk of credit card fraud.

There is also a magnitude of risk from outside the enterprise. For example, every year numerous companies and government agencies fall prey to nefarious hackers. Far too frequently, these unscrupulous hackers are successful in gaining access to credit card information stored in corporate databases. A prominent recent example is the compromise of customer credit card information stored through the PlayStation Network by Sony Corporation. [ii] Statistic Brain, an organization that brings timely and accurate statistics to the public domain released a report in July 2012 pertaining to this issue. Highlights of the report are:

- Percent of Americans who have been victims of credit card fraud: **10%**
- Percent of all financial fraud related to credit cards: **40%**
- Total amount of credit card fraud worldwide: **$5.55 billion**

[iii] Online Trust Alliance (OTA), an IRS 501(c) 6 nonprofit entity seeking to enhance online trust and safety while promoting innovation, reports that in 2012, 2,644 breaches were reported worldwide. This marked an increase of over 117% from 2011, and the total number of records exposed was over 267 million. The direct and indirect costs of such breaches can be staggering.

The PCI DSS Council was set up to define, update, and maintain PCI data security standards to help organizations increase controls and protect customer's payment related information to prevent incidences such as those discussed above.

While achieving PCI compliance is a vital goal, a well-architected payment automation solution can help companies streamline their payments-related business processes, improve the productivity of accounts receivable (AR) and customer service (CS) functions, and potentially reduce credit cards processing fees.

The full lifecycle of a credit card and/or EFT transaction is a veritable cornucopia of complexity due to:

- Security concerns while sensitive information is being routed through multiple agencies
- The need for collaboration with multiple agencies
- High costs and other consequences of errors
- Potential time lag between the authorization process (first step) and the final settlement

Figure 1 provides an overarching view of the various entities that participate in the payment process:

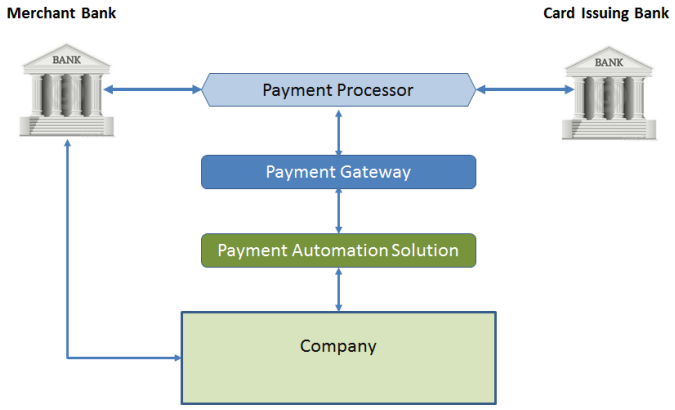

Figure1: Payment Processing Entities