

# PAYMENT VENDORS

## *HOW TO CHOOSE THE RIGHT ONES*

---

---

This document is to help merchants find the most qualified payment applications and service providers to use. If you want to learn more about PCI Compliance, check out our whitepaper: [PCI Compliance: What It Is And How To Maintain It](#)

## INTRODUCTION

If you are currently processing electronic payments or you are looking into doing so in the future, one of the most important things to keep in mind is finding the best payment applications and service providers to help you process those payments.

According to the Payment Card Industry, a payment application is any hardware or software that processes, transmits or stores card data electronically. A few examples of payment applications are card swipe terminals, eCommerce/webstores, and online bill pay portals.

A service provider is a business entity that is directly involved in the processing, transmitting, and storage of cardholder data but is not a payment brand. A few examples of service providers are hosting providers and entities providing managed services like firewalls.

When looking into developing a payment process for your company, you need to consider how you are going to collect the payment data, how you are going to process it, and where you are going to store it. Luckily for merchants, the Payment Card Industry has developed a set of requirements and coinciding certifications for payment vendors and service providers, which helps merchants choose the most qualified solutions and services to use within their organization.

We have put together a list of requirements and certifications from PCI that you should review with your current or potential payment vendors to ensure that you are properly securing your customers' card data.

## Types of Payment Vendors

What do you want to do?	Payment vendor/service provider that you will need	PCI Standard or Certification that you should look for	Where to find their validation
Process, store, and/or transmit cardholder data	Payment Application Vendor	Payment Application Data Security Standard (PA-DSS)	<a href="#">PCI PA-DSS List of Validated Payment Applications</a>
Accept card payments through hardware terminal devices	Payment Terminal Vendor	PIN Transaction Security (PTS)	<a href="#">PCI List of Approved PTS Devices</a>
Use a cloud-based payment application	Software as a Service Providers	PCI DSS	Provider must have a PCI DSS Attestation of Compliance and be on one of the following lists: <a href="#">Compliant Service Providers – MasterCard</a> <a href="#">Compliance Service Providers – Visa</a>



## QUESTIONS TO ASK YOUR PAYMENT VENDORS

Once you are aware of the types of vendors you will need to help you through your payment collection process, you can verify your potential vendors with the following questions.

1. Where does your solution store the payment card data?

If the answer is:

- Locally – Ask question 2
- Off-Site – Ask question 3

2. Is it PA-DSS certified?

If the answer is:

- Yes - check to see if solution is on [PCI PA-DSS List of Validated Payment Applications](#)
- No - look for another payment application vendor who is certified

3. Is the location of the off-site payment storage PCI-DSS certified?

If the answer is:

- Yes - ask the vendor for their PCI DSS Attestation of Compliance and check that they are on one of the following lists:  
[List of Compliant Service Providers – MasterCard](#)  
[List of Compliance Service Providers – Visa](#)
- No - look for another payment application vendor who is certified



## HOW NODUS CAN HELP

Nodus takes payment security and PCI compliance very seriously. All of Nodus' payment applications are PA-DSS certified, and we ensure that every version of our solutions has been tested and validated before we release it to our customers.

Besides our ePayment processing, online bill pay, and eCommerce solutions, Nodus offers a few additional solutions to help merchants protect the payment data that they are processing and storing.

# 1

## Point-of-Entry

Nodus PayFabric has been integrated with certain card readers to provide merchants the ability to accept EMV in addition to the traditional magnetic stripe information. One device we support is PAX S300, a retail smart PINpad that encrypts and protects all transaction information. We also support the PAX D210, a mobile payment device that interacts with customers via Bluetooth, WiFi, or cable connection. This device has state of the art security functions and has been certified through the PCI Security Council.

The PAX S300 and PAX D210 devices are on [PCI's list of Approved PTS Devices](#)

PTS requirements ensure a hardware device helps a merchant's PCI DSS compliance efforts. With PTS approved devices, it's much easier for merchants to secure sensitive card data at the point of interaction, so that in combination with PCI DSS and PA-DSS, the processing, transmitting and storage of account data is better protected.

# 2

## Storage

Nodus PayFabric is a cloud-based storage engine that removes sensitive credit card data from the merchant's environment and stores it off-site in the cloud. It also uses an iframe to pull the credit card information directly from the point-of-entry, preventing the credit card number from ever even touching your application or database.

PayFabric is PCI DSS Level 1 Compliant:

[PCI DSS Certificate of Validation](#)

[PCI DSS Attestation of Compliance](#)

[ASV PCI Scan Attestation of Compliance](#)

[PayFabric's PCI DSS listings for MasterCard](#)

[PayFabric's PCI DSS listings for Visa](#)

# 3

## Point-to-Point Encryption

Another concern is having the credit card information entered into an organization's system unencrypted. Nodus has partnered with Bluefin payment systems, who specializes in integrated payment and P2PE (Point-to-Point Encryption) security technology. Using Bluefin's P2PE supported device, merchants can further enhance the security at the point-of-entry by encrypting the data as soon as it is collected.

Bluefin P2PE is a PCI certified Point-to-Point Encryption solution. Check out their validation here: [PCI Point-to-Point Encryption Solution](#)

## REMEMBER

PCI compliance is *not* a one-time task. In order to provide maximum security of cardholder data, a merchant should continuously monitor and enforce the Payment Card Industry Security Standards.



## Nodus Technologies, Inc.

Nodus Technologies provides businesses and developers with integrated payment solutions for Microsoft Dynamics ERPs and CRM, on-premises or in the cloud. Our expertise in electronic payment processing, B2B & B2C eCommerce, online bill pay, and cloud payment solutions assists organizations of any size and industry with achieving PCI compliance while automating accounts receivables, expediting funding, and improving the customer experience.

Nodus can help merchants obtain PCI Compliance by providing certified payment applications, P2PE and EMV-supported devices, and cloud-based processing and storage technology.

### Contact Us



(909)-482-4701



[sales@nodus.com](mailto:sales@nodus.com)



[www.nodus.com](http://www.nodus.com)