



## *CORPORATE HEADQUARTERS*

100 New Britain Boulevard  
Chalfont, PA 18914-1832  
Phone: 215-997-8989  
Fax: 215-997-3919  
Email: datacap@dcap.com

---

## **Datacap PCI EZ-Validation Program Program Overview**

To protect and prevent fraudulent use of cardholder data, payment card industry (PCI) requirements implemented over the past few years mandate that all POS/ECR payment applications meet PCI PABP or PA-DSS requirements and be validated as such. Card payment services (acquirers, processors, ISOs, etc) are already tasked with insuring that new merchant customers are PCI compliant or using validated POS solutions to accept them as customers. Furthermore, the payment services are required to confirm by July 1, 2010 that all of their customers are doing so, and must stop processing for any who are not meeting the requirements. Compliance and validation adds a significant, unavoidable cost burden to POS system developers, and there are high risks associated with not complying and with not being validated. Furthermore, the costs of both validation and non-validation are certain to increase in the future, as the security standards become more complex and as compliance and validation become more important to retailers. To help POS software developers with PCI issues, Datacap has collaborated with 403 Labs to offer the Datacap PCI EZ-Validation Program, designed to simplify and streamline the PCI validation effort and the associated expense incurred by participating software developers.

The Datacap PCI EZ-Validation program leverages Datacap's own PCI validations, to provide POS/ECR software developers using Datacap payment solutions a streamlined and cost effective way to have their applications validated against the PA-DSS standard by 403 Labs. 403 Labs is a leader in secure validation of PC-based and embedded non-PC POS applications. POS applications using Datacap pay solutions and meeting the associated requirements can be assessed and validated by 403 Labs quickly at a very discounted rate. Datacap and 403 Labs have worked closely together to provide a validation foundation and to thoroughly familiarize 403 Labs with Datacap's integrated payment products and services, and with their use in integrated environments. This experience and knowledgebase enables 403 Labs to perform Datacap partner validations efficiently, and to pass the cost savings on to Datacap payment product users. These efficiencies can translate to validation savings of 50% or more for Datacap partners.

### **How Does the Program Work?**

POS and ECR developers who wish to participate in the program should contact 403 Labs and indicate they are interested in participating in the Datacap PCI EZ-Validation Program. Phone the 403 Labs' Sales Department in Milwaukee at (877) 403-5227.

You will be asked the questions indicated below to determine the characteristics of your application (that is, how it handles card data), and how it fits the PCI PA-DSS assessment criteria. 403 Labs will then review the responses to these questions, and classify your

application into one of a few category tiers, depending on how your application receives, handles and stores cardholder data. They will tell you that either you qualify for the specialized discounted assessment and validation, or that a more extensive validation is required (and the extent of the assessment required), or that they feel no validation is currently required.

If you qualify for the special Datacap program discounted assessment and validation, 403 Labs will prepare a proposal outlining the assessment project for you to review and sign, and will work with you to schedule the project. You will need to provide a system for them to test. When the project begins, they will work with you remotely to review your application against the PCI PA-DSS criteria (against the 14 major requirements, which are outlined below). You will need to make any changes they may indicate to become compliant. Once all the gaps identified in the assessment have been remediated (taken care of or corrected), 403 Labs will submit a Report on Validation (ROV) to the PCI Security Standards Council for their approval. Once PCI approves the ROV, your application is eligible to be added to the PCI PA-DSS Approved Application list, upon payment of the PCI Security Standards Council's listing fees (currently \$1,250 per POS software application). Under the Datacap EZ-Validation program, typically POS developers using Tran™ products will pay \$5,000 for the program assessment and validation, and NETePay™/DIALePay™ (DSIClientx™) developers will pay \$6,000. This compares to typical standard assessment fees of \$10-14,000 or more. Multi-product discounts are available, and multi-year testing/assessment agreements can also reduce assessment expenses even more in the long term.

If your application requires a more extensive assessment and validation, 403 Labs will ask additional scoping questions to get a better feel for the application and provide you a customized proposal and quotation based on the structure and size of your application. Otherwise the process above will apply.

## **Payment Application Data Security Standards (PA-DSS) Criteria**

The PCI Security Assessment performed by 403 Labs will address the requirements of the Payment Card Industry Payment Application Data Security Standards as defined by the PCI Security Standards Council. POS/ECR software application creation and maintenance design and development practices are evaluated, working towards PCI's stated PA-DSS goal "to ensure the application does not retain full magnetic stripe data or CVV data and that it supports a merchant's and service provider's ability to comply with the PCI Data Security Standard." Toward this goal, the assessment team will evaluate the application against the 14 major PA-DSS requirements:

1. Never retain full magnetic stripe, card validation codes/values (CVV, CVC, CID, CAV), or PIN block data
2. Protect stored cardholder data
3. Provide secure password features
4. Log application activity
5. Develop secure applications
6. Protect wireless transmissions
7. Test applications to address vulnerabilities
8. Facilitate secure network implementation
9. Cardholder data must never be stored on a server connected to the Internet
10. Facilitate secure remote software updates
11. Facilitate secure remote access to application
12. Encrypt sensitive traffic over public networks
13. Encrypt all non-console administrative access
14. Maintain instructional documentation and training programs for customers, resellers, and integrators

## Initial Scoping Questions to Classify an Application into Tiers

The questions initially asked to determine whether the POS application falls within the criteria of the streamlined, discounted Datacap PCI assessment and validation program are:

1. Does the application perform card-present transactions (i.e., face to face), card-not-present transactions (e.g., telephone order or e-commerce), or both?
2. Does the application accept card data via manual entry or an on-board magnetic stripe reader and then pass it to a Datacap device or software?
3. Does the application store any cardholder data, even for short periods of time, independent of the Datacap device's card data storage?
4. Does the application either store sensitive authentication data (e.g., magnetic stripe data or card verification numbers) beyond the length of time required to authorize the transactions? or have prior versions ever done so?
5. Does the application connect only to a Datacap device or can it connect to other systems or networks?
6. Does the application provide or make use of remote access such as a virtual private network (VPN), pcAnywhere, or LogMeIn?

## What Information will I the developer need to provide?

The PCI security assessment and validation is a cooperative effort between you the POS developer, 403 Labs and Datacap. The 403 Labs assessment team will need your cooperation and access to view and review all application specifications.

The information and documentation you will need to provide includes:

1. A description of all application components (hardware and software)
2. An example of a typical installation including written description and a network diagram
3. Since this assessment is being done remotely, you'll need to send 403 Labs a complete installation system, including all materials required to reproduce a typical installation in the 403 Labs testing lab. Of course, this will be returned to you at the end of the project.
4. A diagram detailing card data flow
5. Software development life cycle policy and relevant software development procedures
6. An explanation of your secure coding practices, including references to third-party guidelines (e.g., OWASP) as well as how these are incorporated into development efforts. Also, any training materials on secure coding education.
7. A sample of change control documentation
8. A sample of code review documentation
9. A sample of security testing documentation
10. Implementation guidelines for customers and resellers as appropriate
11. Training materials for resellers or VARs/systems integrators

And as the assessment commences, 403 Labs will advise you of any additional information or documentation required.

## Let's Get Started

That covers the key points of the Datacap PCI EZ-Validation program, intended to keep card data safe and make your validation effort faster and less expensive, just because you are using Datacap payment interfaces. Validated applications are easier to sell, and protect your customers and their customers. If there are questions, feel free to call Datacap or 403 Labs at any time.