

FLORIDA DEPARTMENT OF TRANSPORTATION



RFP-DOT- 09/10-8001-KB

PAYMENT CARD INDUSTRY (PCI) SERVICES

FPI No. 423249-1-32-01

ADVERTISEMENT

REQUEST FOR PROPOSAL STATE OF FLORIDA DEPARTMENT OF TRANSPORTATION FLORIDA'S TURNPIKE ENTERPRISE

Sealed Request for Proposals will be received by the Department of Transportation, Florida's Turnpike Enterprise, Contractual Services Office, Building 5315 on Florida's Turnpike, Milepost 263.0, Turkey Lake Service Plaza, Ocoee, Florida, 34761, until **2:30 P.M. (eastern standard time) on August 25, 2009**, for the following project:

BID NO. RFP-DOT-09/10-8001-KB

SCOPE OF SERVICES: The Florida Department of Transportation, Florida's Turnpike Enterprise (hereinafter referred to as the "Department") under this agreement requires a Vendor that is recognized and approved by the PCI Security Standards Council to provide Payment Card Industry (PCI) required services for a Level 1 merchant. These services will be required on an annual basis. Any additional services above and beyond the minimum PCI Data Security Standards (DSS) to ensure an annual passing report of compliance are welcomed.

Vendor's Qualifications

The Vendor shall maintain and keep in force throughout the life of the contract, renewals and any extensions, the requirements specified below. Failure of the Vendor to comply with these requirements will be sufficient ground for the Turnpike District to declare the contract in default subject to the terms of Section 6, Termination and Default, of the Standard Written Agreement.

1. Vendor must be or employ a PCI Qualified Security Assessor (QSA), PCI Approved Scanning Vendor (ASV) and a qualified forensic expert that is a Visa-approved Qualified Incident Response Assessor (QIRA). All subcontractors must be approved by the Department.
2. Vendor must be qualified to do business in the State of Florida.
3. All work performed must be in accordance with PCI specified procedures for the PCI annual onsite security audit.
4. PCI specified procedures for meeting or exceeding the PCI DSS Requirement 11.2, 11.3, 11.3.1, 11.3.2 and 6.6 with tests that include the vulnerabilities listed in Requirement 6.5. (Attachment B)
5. All deliverables must be in accordance with PCI specified requirements with all reports being acceptable by the onsite PCI auditor and acquiring bank.
6. All work performed and deliverables must be kept confidential per a non-disclosure agreement. (Attachment A)

The Department will investigate carefully to determine if the vendor is responsive, responsible and qualified in the area of work contemplated by this contract.

HOW TO APPLY: Prospective bidders may request and obtain a complete Request for Proposal (RFP), including specifications and general proposal conditions for the above-referenced project at no cost, by e-mailing their name, address, telephone number and fax number to Ms. Karen Bracy, FDOT Turnpike Enterprise, at karen.brac@dot.state.fl.us. **Please reference the RFP number in the subject box when ordering.**

MANDATORY PRE-PROPOSAL MEETING: The Department will convene a **MANDATORY PRE-PROPOSAL MEETING** for this Request for Proposal (RFP) on August 10, 2009, at 01:00 P.M. The Proposer's have three (3) options. The meeting will be held via video conference in the Turnpike Enterprise Office, located on Florida's Turnpike M.P. 263, Turkey Lake Service Plaza Bldg. 5315, Room 3163, (407)-532-3999 and the Turnpike SunPass® Service Center, 7941 Glades Road, Boca Raton, Florida 33434, Room 136, (561) 470-6600. The meeting will also be assessable via teleconference on (850) 414-4976. **FAILURE OF A PROPOSER TO BE IN ATTENDANCE, AT ONE OF THE LOCATIONS MENTIONED OR CONNECT TO THE TELECONFERENCE, FOR THE MANDATORY PRE-PROPOSAL MEETING WILL RESULT IN REJECTION OF THE PROPOSAL.**

The Department reserves the right to reject any or all proposals.

NOTE: All of the Department's **ITB/RFP/ITN ADVERTISEMENTS** appear on the Internet at website:

<http://myflorida.com>

Click on "Business"

Click on "Doing Business with the State"

Under "Everything for Vendors and Customers" Click on "Vendor Bid System (VBS)"

Under "Vendor Bid System" Click on "Search Advertisements"

Drop menu for Agency and Select "Department of Transportation"

Scroll down and Click on "Initiate Search"

We encourage all vendors to regularly check this site.

State of Florida
Department of Transportation
Florida's Turnpike Enterprise
Contractual Services Office
P. O. Box 613069
Ocoee, Florida 34761- 3069

REQUEST FOR PROPOSAL REGISTRATION

ALL VENDORS MUST COMPLETE AND RETURN THIS FORM TO THE ABOVE ADDRESS OR FAX TO:
(407) 822-5821, ATTN: KAREN BRACY

ITB Number: RFP-DOT-09/10-8001-KB

Title: PAYMENT CARD INDUSTRY (PCI) SERVICES

Proposal Due Date and Time: AUGUST 25, 2009 at 2:30 PM (Eastern Standard Time)

Potential Proposers should notify our office by returning this Proposal Registration Form as soon as possible after downloading. Complete the information below and fax **this sheet only** to the Florida Department of Transportation Procurement Office at 407-822-5821, or mail to the address noted above.

THE REQUEST FOR PROPOSAL DOCUMENT YOU RECEIVED IS SUBJECT TO CHANGE. Notice of changes (addenda), will be posted on the Florida Vendor Bid System at www.myflorida.com, under this proposal number (click on "BUSINESS", click on "Doing Business with the State", under "Everything for Vendors and Customers", click on "Vendor Bid System (VBS)", then click on "Search Advertisements", click on the drop-down arrow beside the box under Advertisement Type, select Competitive Solicitation, click on the drop-down arrow beside the box under Agency, select DEPARTMENT OF TRANSPORTATION, then go to the bottom of the same page and click on Initiate Search). It is the responsibility of all potential bidders to monitor this site for any changing information prior to submitting your bid.

Business Name: _____

Address: _____

City, State, Zip: _____

Telephone: (____) _____ Fax Number: (____) _____

Contact Person: _____

Internet E-Mail Address: _____

For further information on this process, you may e-mail or telephone: Karen Bracy at Karen.bracy@dot.state.fl.us or 407-264-3696

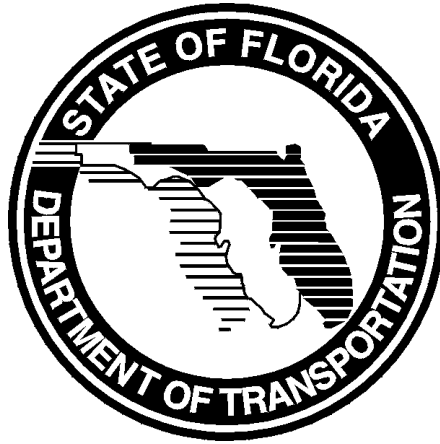


TABLE OF CONTENTS

RFP-DOT- 09/10-8001-KB

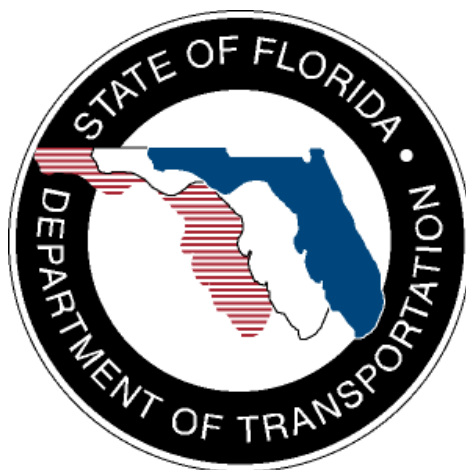
PAYMENT CARD INDUSTRY (PCI) SERVICES

FPI No. 423249-1-32-01

Table of Contents

<u>ITEM</u>	<u>PAGE NO.</u>
Cover Sheet	
Advertisement	
Request for Proposal	
Table of Contents.....	TOC 1
Request for Proposal Instructions (Special Conditions)	SC1-SC13
General Contract Conditions (PUR 1000).....	1-10
General Instructions to Respondents (PUR 1001).....	1-5
Forms	FORMS 1-4
Standard Written Agreement.....	SWA 1-7
Exhibit "A" Scope of Services.....	1 – 15
Attachments	A - E
Exhibit “B” Method of Compensation.....	1 - 4
Exhibit “C” Price Proposal.....	1 – 8

**State of Florida
Department of Transportation**



INVITATION TO BID

**ITB-DOT-09/10-8001-KB
PAYMENT CARD INDUSTRY (PCI) SERVICES**

FPI No. 423249-1-32-01

MAIL BIDS, ADMINISTRATIVE AND TECHNICAL QUESTIONS TO:

**Ms. Karen Bracy
Florida Department of Transportation
Florida's Turnpike Enterprise
P. O. Box 613069
Ocoee, FL 34761-3069
Phone: (407) 264-3696
Fax: (407) 822-5821
Email: karen.bracy@dot.state.fl.us**

SUBMIT SEALED BIDS VIA OVERNIGHT MAIL OR HAND DELIVERY TO:

**Ms. Karen Bracy
Florida's Turnpike Enterprise
Florida's Turnpike, Milepost 263.0
Building No., 5315, Turkey Lake Service Plaza
Ocoee, Florida 34761-3069**

INTRODUCTION SECTION

1) INVITATION

The State of Florida Department of Transportation hereinafter referred to as the “Department”, requests written proposals from qualified Proposers to provide Payment Card Industry required services for a Level 1 merchant. The term of the contract will be three (3) years anticipated to begin the third quarter of 2009.

The Department intends to award this contract to the responsive and responsible Proposer whose proposal is determined to be the most advantageous to the Department. After the award, said Proposer will be referred to as the “Vendor”. For the purpose of this document, the term "Proposer" means the prime Vendor acting on its own behalf and those individuals, partnerships, firms, or corporations comprising the Proposer team. The term "proposal" means the complete response of the Proposer to the Request for Proposals (RFP), including properly completed forms and supporting documentation.

2) COORDINATION OR PROCUREMENT AND CONTRACT DOCUMENTS

This solicitation consists of the contract documents identified below which are integral parts of the Contract and as such, a requirement occurring in one is as binding as though occurring in all. All parts of the Contract are complimentary and establish the procurement process and describe and provide for complete work. In case of discrepancy, the governing order of the contract documents is as follows:

1. Standard Written Agreement (when executed)
2. Special Conditions
3. Exhibit “A” - Scope of Services
4. Exhibit “B” – Method of Compensation
5. Exhibit “C” – Price Proposal
6. Attachments A - E
7. State of Florida PUR 1000 General Contract Conditions
8. State of Florida PUR 1001 General Instructions to Respondents

SPECIAL CONDITIONS

1) MyFloridaMarketPlace

Since July 1, 2003, the Department has been using the State of Florida's web-based electronic procurement system, MyFloridaMarketPlace. PROPOSERS MUST BE REGISTERED IN THE STATE OF FLORIDA'S MYFLORIDAMARKETPLACE SYSTEM BY THE TIME AND DATE OF THE TECHNICAL PROPOSAL OPENING OR THEY WILL BE CONSIDERED NON-RESPONSIVE (see Special Condition 21). All prospective proposers that are not registered should go to <https://vendor.myfloridamarketplace.com/> to complete on-line registration, or call 1-866-352-3776 for assisted registration.

2) QUESTIONS & ANSWERS

In accordance with section 287.057(24), Florida Statutes, respondents to this solicitation or persons acting on their behalf may not contact, between the release of the solicitation and the end of the 72-hour period following the agency posting the notice of intended award, excluding Saturdays, Sundays, and state holidays, any employee or officer of the executive or legislative branch concerning any aspect of this solicitation, except in writing to the procurement officer or as provided in the solicitation documents. Violation of this provision may be grounds for rejecting a response.

Any technical questions arising from this Request for Proposal must be forwarded, in writing, to the procurement agent identified below. Questions must be received no later than the time and date reflected on the SCHEDULE OF EVENTS. The Department's written response to written inquiries submitted timely by proposers will be posted on the Florida Vendor Bid System at www.myflorida.com (click on "BUSINESS", click on "Doing Business with the State", under "Everything for Vendors and Customers", click on "Vendor Bid System (VBS)", click on "Search Advertisements"), under this RFP number. It is the responsibility of all potential proposers to monitor this site for any changing information prior to submitting their proposal.

WRITTEN TECHNICAL QUESTIONS should be submitted to:

Karen Bracy, karen.bracy@dot.state.fl.us, Florida's Turnpike, Milepost 263.0, Turkey Lake Service Plaza, Building 5315, Ocoee, FL 34761, with the RFP-DOT-09/10-8001-KB listed in the subject box.

Questions regarding administrative aspects of the proposal process should be directed to the Karen Bracy in writing at the address above or by phone: phone number (407) 264-3696, fax number (407) 822-5821.

3) ORAL INSTRUCTIONS / CHANGES TO THE REQUEST FOR PROPOSAL (ADDENDA)

No negotiations, decisions, or actions will be initiated or executed by a proposer as a result of any oral discussions with a State employee. Only those communications which are in writing from the Department will be considered as a duly authorized expression on behalf of the Department.

Notices of changes (addenda) will be posted on the Florida Vendor Bid System at www.myflorida.com (click on "BUSINESS", click on "Doing Business with the State", under "Everything for Vendors and Customers", click on "Vendor Bid System (VBS)", click on "Search Advertisements") under this RFP number. It is the responsibility of all potential proposers to monitor this site for any changing information prior to submitting your proposal. All addenda will be acknowledged by signature and subsequent submission of addenda with proposal when so stated in the addenda.

4) MINORITY BUSINESS ENTERPRISE (MBE) UTILIZATION

The Department encourages small, minority, women, and service-disabled veteran businesses to compete for Department contracts, both as "Vendor" and as subcontractors. The Department, its vendors, suppliers, and consultants should take all

necessary and reasonable steps to ensure that small, minority, women, and service-disabled veteran businesses have the opportunity to compete for and perform contract work for the Department in a nondiscriminatory environment.

To request certification or to locate certified MBEs, call the Office of Supplier Diversity, Department of Management Services at (850) 487-0915, or access their MBE directory on the Internet at www.osd.dms.state.fl.us/.

5) SCHEDULE OF EVENTS

Provided below is a list of critical dates and actions. These dates are subject to change. Notices of changes (addenda) will be posted on the Florida Vendor Bid System at www.myflorida.com (click on “BUSINESS”, click on “Doing Business with the State”, under “Everything for Vendors and Customers”, click on “Vendor Bid System (VBS)”, click on “Search Advertisements”) under this RFP number. It is the responsibility of all potential proposers to monitor this site for any changing information prior to submitting your proposal.

ACTIVITY	DATE	LOCATION/TIME
Mandatory Pre-Proposal Video and Telephone Conference For Interested Firms (Notes 3)	August 10, 2009	Turnpike Enterprise Headquarters Room 3163, Turnpike SunPass Service Center Room 136 at 01:00 p.m. or 850-414-4976 (Note 2 and Note 4))
Deadline for Technical Questions	August 18, 2009	Via email to karen.bracy@dot.state.fl.us by 5:00 p.m.
Submission of Sealed Proposals (Technical & Price proposals in separate sealed packages) (Note 1)	Tuesday, August 25, 2009	Turnpike Enterprise Headquarters at 2:30 p.m. (Note 2)
Opening of Sealed Technical Proposals (Notes 3)	Tuesday, August 25, 2009	Turnpike Enterprise Headquarters at 2:30 p.m. (Note 2)
Opening of Price Proposals (Notes 3)	Tuesday, September 1, 2009	Turnpike Enterprise Headquarters at 2:30 p.m. (Note 2)
Posting of Intended Award	Tuesday, September 8, 2009 through Friday, September 11, 2009	VBS/Internet at 4:30 p.m.

NOTES:

Note 1 - It is the proposer’s responsibility to assure that the bid is delivered to the proper place on or before the Bid Due date and time. Bids which for any reason are not so delivered will not be considered.

Note 2 – The Turnpike Enterprise Headquarters address is **Florida’s Turnpike M.P. 263.0, Turkey Lake Service Plaza, Ocoee, Florida 34761.**

Note 3 - All meetings listed in the Schedule of Events, are open to the public.

Note 4 – The Turnpike SunPass Service Center address is **7941 Glades Road, Boca Raton, Florida 33434.**

6) SPECIAL ACCOMMODATIONS

Any person with a qualified disability requiring special accommodations at a pre-proposal conference, public meeting, oral presentation and/or opening shall contact the contact person at the phone number, e-mail address or fax number provided on the title page at least five (5) working days prior to the event. If you are hearing or speech impaired, please contact this office by using the Florida Relay Services which can be reached at 1 (800) 955-8771 (TDD).

7) SCOPE OF SERVICES

Details of the services, information and items to be furnished by the Vendor are described in Exhibit "A", Scope of Services, attached hereto and made a part hereof.

8) INTENDED AWARD

The Department intends to award a contract to the responsive and responsible vendor with the highest cumulative total points for the evaluation criteria specified herein (See Section 30, Proposal Evaluation). The Intended Award decision will be announced after final evaluation and totaling of scores at the Price Proposal opening specified in the SCHEDULE OF EVENTS. If the Department is confronted with identical pricing or scoring from multiple vendors, the Department shall determine the order of award in accordance with Rule 60A-1.011 Florida Administrative Code.

9) MANDATORY PRE-PROPOSAL CONFERENCE

A MANDATORY pre-proposal conference will be held at the date, time and location in the SCHEDULE OF EVENTS. The purpose of this meeting is to provide an open forum for the Department to review the Scope of Services and respond to questions from potential proposers regarding the scope of services, RFP requirements, contractual requirements, method of compensation, and other conditions or requirements that may, in any manner, effect the work to be performed. Any changes and/or resulting addenda to the RFP will be the sole prerogative of the Department.

Attendance at this pre-proposal conference is MANDATORY. Failure by a proposer to attend, be represented or connect to the teleconference for this pre-proposal conference will constitute a non-responsive determination of their proposal package. Proposals found to be non-responsive will not be considered.

10) QUALIFICATIONS

10.1 General

The Department will determine whether the Proposer is qualified to perform the services being contracted based upon their proposal demonstrating satisfactory experience and capability in the work area. The Proposer shall identify necessary experienced personnel and facilities to support the activities associated with this proposal.

10.2 Qualifications of Key Personnel

Those individuals who will be directly involved in the project should have demonstrated experience in the areas delineated in the scope of work. Individuals whose qualifications are presented will be committed to the project for its duration unless otherwise determined by the Department's Project Manager. Where State of Florida registration or certification is deemed appropriate, a copy of the registration or certificate should be included in the proposal package.

10.3 Authorized To Do Business in the State of Florida

In accordance with sections 607.1501, 608.501, and 620.169, Florida Statutes, foreign corporations, foreign limited liability companies, and foreign limited partnerships must be authorized to do business in the State of Florida. Such authorization should be obtained by the proposal due date and time, but in any case, must be obtained prior to posting of the intended award of the contract. For authorization, contact:

Florida Department of State
Tallahassee, Florida 32399
(850) 245-6051

10.4 Licensed to Conduct Business in the State of Florida

If the business being provided requires that individuals be licensed by the Department of Business and Professional Regulation, such licenses should be obtained by the proposal due date and time, but in any case, must be obtained prior to posting of the intended award of the contract. For licensing, contact:

Florida Department of Business and Professional Regulation
Tallahassee, Florida 32399-0797
(850) 487-1395

11) WARRANTY/SUBSTITUTIONS

When performance of the services requires the supply of commodities, a warranty is required on all items provided against defective materials, workmanship, and failure to perform in accordance with required industry performance criteria, for a period of not less than ninety (90) days from the date of acceptance by the purchaser. Any deviation from this criteria must be documented in the proposal response or the above statement shall prevail. Delivery of substitute commodities requires prior written approval from the ordering location.

Replacement of all materials found defective within the warranty period shall be made without cost to the purchaser, including transportation if applicable. All fees associated with restocking cancelled orders shall be the responsibility of the vendor.

All items provided during the performance of the contract found to be poorly manufactured will not be accepted, but returned to the vendor, at their expense, for replacement. Replacement of all items found defective shall be made without cost to the Department, including transportation, if applicable. As it may be impossible for each facility to inspect all items upon arrival, a reasonable opportunity must be given to these facilities for inspection of the items, and returning those that are defective.

12) LIABILITY INSURANCE

(X) No general liability insurance is required.

13) PERFORMANCE BOND

(X) No Performance Bond is required for this project.

14) METHOD OF COMPENSATION

Details of the method of compensation, for the Vendor are described in Exhibit "B", Method of Compensation, attached hereto and made a part hereof.

15) CONTRACT DOCUMENT

STANDARD WRITTEN AGREEMENT

The Department's "Standard Written Agreement" is attached hereto and made a part hereof. The terms and conditions contained therein will become an integral part of the contract resulting from this solicitation. In submitting a proposal, the proposer agrees to be legally bound by these terms and conditions.

16) REVIEW OF PROPOSER'S FACILITIES & QUALIFICATIONS

After the proposal due date and prior to contract execution, the Department reserves the right to perform or have performed, an on-site review of the Proposer's facilities and qualifications. This review will serve to verify data and representations submitted by the Proposer and may be used to determine whether the Proposer has an adequate, qualified, and experienced staff, and can provide overall management facilities. The review may also serve to verify whether the Proposer has financial capability adequate to meet the contract requirements.

Should the Department determine that the proposal has material misrepresentations or that the size or nature of the Proposer's facilities or the number of experienced personnel (including technical staff) are not adequate to ensure satisfactory contract performance, the Department has the right to reject the proposal.

17) PROTEST OF REQUEST FOR PROPOSAL SPECIFICATIONS

Any person who is adversely affected by the contents of this Request for Proposal must file the following with the Department of Transportation, Clerk of Agency Proceedings, 605 Suwannee Street, Mail Station 58, Room 550, Tallahassee, Florida 32399-0450:

1. A written notice of protest within seventy-two (72) hours after the posting of the solicitation, and
2. A formal written protest in compliance with Section 120.57(3), Florida Statutes, within ten (10) days of the date on which the written notice of protest is filed.

Failure to file a protest within the time prescribed in section 120.57(3), Florida Statutes, or failure to post the bond or other security required by law within the time allowed for filing a bond shall constitute a waiver of proceedings under Chapter 120, Florida Statutes.

18) UNAUTHORIZED ALIENS

The employment of unauthorized aliens by any contractor is considered a violation of Section 274A(e) of the Immigration and Nationality Act. If the contractor knowingly employs unauthorized aliens, such violation shall be cause for unilateral cancellation of the contract.

19) RESERVATIONS

The Department reserves the right to accept or reject any or all proposals received and reserves the right to make an award without further discussion of the proposals submitted. Therefore, the proposals should be submitted initially in the most favorable manner. It is understood that the proposal will become a part of the Department's official file, without obligation to the Department.

20) ADDITIONAL TERMS & CONDITIONS

No conditions may be applied to any aspect of the RFP by the proposer. Any conditions placed on any aspect of the proposal documents by the proposer may result in the proposal being rejected as a conditional proposal (see "RESPONSIVENESS OF PROPOSALS"). **DO NOT WRITE IN CHANGES ON ANY RFP SHEET.** The only recognized changes to the RFP prior to proposal opening will be a written addenda issued by the Department.

21) RESPONSIVENESS OF PROPOSALS

21.1 Responsiveness of Proposals

Proposals will not be considered if not received by the Department on or before the date and time specified as the due date for submission.

All proposals must be typed or printed in ink. A responsive proposal is an offer to perform the scope of services called for in this Request for Proposal in accordance with all requirements of this Request for Proposal. Proposals found to be non-responsive shall not be considered. Proposals may be rejected if found to be irregular or not in conformance with the requirements and instructions herein contained. A proposal may be found to be irregular or non-responsive by reasons, that include, but are not limited to, failure to utilize or complete prescribed forms, conditional proposals, incomplete proposals, indefinite or ambiguous proposals, and improper and/or undated signatures.

21.2 Multiple Proposals

Proposals may be rejected if more than one proposal is received from a Proposer. Such duplicate interest may cause the rejection of all proposals in which such Proposer has participated. Subcontractors may appear in more than one proposal.

21.3 Other Conditions

Other conditions which may cause rejection of proposals include, but are not limited to, evidence of collusion among Proposers, obvious lack of experience or expertise to perform the required work, failure to perform or meet financial obligations on previous contracts, or in the event an individual, firm, partnership, or corporation is on the United States Comptroller General's List of Ineligible Contractors for Federally Financed or Assisted Projects.

22) PROPOSAL FORMAT INSTRUCTIONS

22.1 General Information

This section contains instructions that describe the required format for the proposal. All proposals submitted shall contain two parts and be marked as follows:

PART I TECHNICAL PROPOSAL NUMBER RFP-DOT-09/10-8001-KB
(One Separately Sealed Package for Technicals)

PART II PRICE PROPOSAL NUMBER RFP-DOT-09/10-8001-KB
(One Separately Sealed Package for Prices)

THE SEPARATELY SEALED PACKAGES MAY BE MAILED TOGETHER IN ONE ENVELOPE OR BOX.

22.2 Technical Proposal (Part I) (4 copies and 1 original) (Do not include price information in Part I)

The Proposer must submit (4) copies and one (1) original of the technical proposal which are to be divided into the sections described below. Since the Department will expect all technical proposals to be in this format, failure of the Proposer to follow this outline may result in the rejection of the proposal. The technical proposal must be submitted in a separate sealed package marked "TECHNICAL PROPOSAL NUMBER RFP-DOT-09/10-8001-KB".

1. EXECUTIVE SUMMARY

The Proposer shall provide an Executive Summary to be written in nontechnical language to summarize the Proposer's overall capabilities and approaches for accomplishing the services specified herein. The Proposer is encouraged to limit the summary to no more than ten (10) pages.

2. PROPOSER'S MANAGEMENT PLAN

The Proposer shall provide a management plan which describes administration, management and key personnel.

a. Administration and Management

The Proposer should include a description of the organizational structure and contract management depth including effectiveness of proposed coordination, measurements of services (Quality Control) and communication between the Department and customers.

b. Identification of Key Personnel

The Proposer should provide the names of key personnel on the Proposer's team, as well as a resume for each individual proposed and a description of the functions and responsibilities of each key person relative to the task to be performed. The approximate percent of time to be devoted exclusively for this project and to the assigned tasks should also be indicated.

3. PROPOSER'S TECHNICAL PLAN

The Proposer shall provide a technical plan which explains the understanding of the technical requirements and the approach used for the proposed services.

a. Understanding the Technical Requirements

The Proposer should explain their overall understanding of the contract requirements for the services and the Personal Confidential Information per PCI Level 1 standards.

b. Proposed Services

The Proposer should explain the overall approach used to accomplish the required tasks based upon the proposed services and specific techniques.

22.3 Price Proposal (Part II) (4 copies and 1 original)

The price proposal information is to be submitted in a separate sealed package marked "PRICE PROPOSAL NUMBER RFP-DOT-09/10-8001-KB". The Price Proposal information shall be submitted on the forms provided in the Request for Proposal.

22.4 Presenting the Proposal

The proposal shall be limited to a page size of eight and one-half by eleven inches (8½" x 11"). Foldout pages may be used, where appropriate, but should not exceed five (5) percent of the total number of pages comprising the proposal. Type size shall not be less than 10 point font. The proposals should be indexed and all pages sequentially numbered. Bindings and covers will be at the Proposer's discretion.

Unnecessarily elaborate special brochures, art work, expensive paper and expensive visual and other presentation aids are neither necessary nor desired.

It is recognized that existing financial reports, documents, or brochures, such as those that delineate the Proposer's general capabilities and experience, may not comply with the prescribed format. It is not the intent to have these documents reformatted and they will be acceptable in their existing form.

23) "DRUG-FREE WORK PLACE" PREFERENCE

Whenever two or more bids which are equal with respect to price, quality, and service are received, the Department shall

determine the order of award in accordance with Rule 60A-1.011 Florida Administrative Code, which includes a preference for bid responses that certify the business has implemented a drug-free workplace program in accordance with Section 287.087, F.S. The "Drug-Free Workplace Program Certification" must be completed and submitted with the bid response for this preference.

24) COPYRIGHTED MATERIAL

Copyrighted material will be accepted as part of a technical proposal only if accompanied by a waiver that will allow the Department to make paper and electronic copies necessary for the use of Department staff and agents. It is noted that copyrighted material is not exempt from the Public Records Law, Chapter 119, Florida Statutes. Therefore, such material will be subject to viewing by the public, but copies of the material will not be provided to the public.

25) ATTACHMENT TO RFP SUBMITTAL - CONFIDENTIAL MATERIAL

The Proposer must include any materials it asserts to be exempted from public disclosure under Chapter 119, Florida Statutes, in a separate bound document labeled "Attachment to Request for Proposals, Number RFP-DOT-09/10-8001-KB Confidential Material". The Proposer must identify the specific Statute that authorizes exemption from the Public Records Law. Any claim of confidentiality on materials the Proposer asserts to be exempt from public disclosure and placed elsewhere in the proposal will be considered waived by the Proposer upon submission, effective after opening.

26) COSTS INCURRED IN RESPONDING

This Request for Proposal does not commit the Department or any other public agency to pay any costs incurred by an individual firm, partnership, or corporation in the submission of a proposal or to make necessary studies or designs for the preparation thereof, nor to procure or contract for any articles or services.

27) MAIL OR DELIVER PROPOSAL TO: (DO NOT FAX)

Florida Department of Transportation
Florida's Turnpike Enterprise
Florida's Turnpike, Milepost 263.0
Building No., 5315, Turkey Lake Service Plaza
Ocoee, Florida 34761-3069
Attn: Karen Bracy
Phone (407) 264-3696

It is the proposer's responsibility to assure that the proposal (Technical and Price proposal) is delivered to the proper place on or before the Proposal Due date and time (See SCHEDULE OF EVENTS). Proposals which for any reason are not so delivered will not be considered.

By submitting a proposal, the Proposer represents that it understands and accepts the terms and conditions to be met and the character, quality and scope of services to be provided.

All proposals and associated forms shall be signed and dated in ink by a duly authorized representative of the Proposer.

Each Proposer shall fully acquaint itself with the conditions relating to the performance of the services under the conditions of this Request for Proposal. This may require an on-site observation.

28) MODIFICATIONS, RESUBMITTAL AND WITHDRAWAL

Proposers may modify submitted proposals at any time prior to the proposal due date. Requests for modification of a

submitted proposal shall be in writing and must be signed by an authorized signatory of the proposer. Upon receipt and acceptance of such a request, the entire proposal will be returned to the proposer and not considered unless resubmitted by the due date and time. Proposers may also send a change in a sealed envelope to be opened at the same time as the proposal. The RFP number, due date and time should appear on the envelope of the modified proposal.

29) PROPOSAL OPENING

All proposal openings are open to the public. Technical Proposals will be opened by the Department at the date, time and location in the SCHEDULE OF EVENTS. Price Proposals, which have a corresponding responsive Technical Proposal, will be opened by the Department at the date, time and location in the SCHEDULE OF EVENTS.

30) PROPOSAL EVALUATION

30.1 Evaluation Process:

A Technical Review team will be established to review and evaluate each proposal submitted in response to this Request for Proposal (RFP). The Technical Review team will be comprised of at least three persons with background, experience, and/or professional credentials in relative service areas.

The Procurement Office will distribute to each member of the Technical Review team a copy of each technical proposal. The Technical Review team members will independently evaluate the proposals on the criteria established in the section below entitled "Criteria for Evaluation" in order to assure that proposals are uniformly rated. The Technical Review team will assign points, utilizing the technical evaluation criteria identified herein and complete a technical summary.

During the process of evaluation, the Procurement Office will conduct examinations of proposals for responsiveness to requirements of the RFP. Those determined to be non-responsive will be automatically rejected.

30.2 Oral Presentations THERE ARE NO ORAL PRESENTATIONS FOR THIS PROJECT.

30.3 Price Proposal

The Proposer shall complete the Price Proposal form and submit as part of the Price Proposal Package. Any proposal in which this form is not used or in which the form is improperly executed may be considered non-responsive and the proposal will be subject to rejection. The vendor's completed form shall become a part of the contract upon award of the contract.

The Procurement Office will open Price Proposals in accordance with Section 29, Proposal Openings. The Procurement Office and/or the Project Manager/Technical Review team will review and evaluate the price proposals and prepare a summary of its price evaluation. The Procurement Office and/or the Project Manager/Technical Review team will assign points based on price evaluation criteria identified herein.

30.4 Criteria for Evaluation

Proposals will be evaluated and graded in accordance with the criteria detailed below.

a. Technical Proposal (70 Points)

Technical evaluation is the process of reviewing the Proposer's Executive Summary, Management Plan, Technical Plan and Assessment Documentation for understanding of project, qualifications, approach and capabilities, to assure a quality product.

The following point system is established for scoring the technical proposals:

	<u>Point Value</u>
1. Executive Summary	5
2. Management Plan	10
3. Technical Plan	40
4. Assessment Documentation	15

b. Price Proposal (30 Points)

Price evaluation (maximum of 30 points) is the process of examining a Proposer's price. The Proposer's price for each year, including the renewals for contract years four (4), five (5), and six (6) will be evaluated using present value methodology as required by section 287.0572(2), Florida Statutes. A present value discount rate of 1.76% shall be used in the evaluation. The price analysis will be conducted by a comparison of the present value of each Proposer's proposal. The criteria for price evaluation shall be based upon the following formula:

$$\frac{(\text{Low Present Value Price} / \text{Proposer's Present Value Price}) \times \text{Price Points (30)}}{= \text{Proposer's Total Price Points}}$$

The lowest present value proposal price will be divided by the Proposer's present value price. The result will be multiplied by the maximum price proposal points (30) to arrive at the total price points for the Proposer.

31) POSTING OF INTENDED AWARD

31.1 The Department's decision will be posted on the Florida Vendor Bid System, at www.myflorida.com, (click on "BUSINESS", click on "Doing Business with the State", under "Everything for Vendors and Customers", click on "Vendor Bid System (VBS)", on date and time in the SCHEDULE OF EVENTS, and will remain posted for a period of seventy-two (72) hours. Any proposer who is adversely affected by the Department's recommended award or intended decision must file the following with the Department of Transportation, Clerk of Agency Proceedings, 605 Suwannee Street, Mail Station 58, Room 550, Tallahassee, Florida 32399-0450:

1. A written notice of protest within seventy-two (72) hours after posting of the Intended Award, and
2. A formal written protest and protest bond in compliance with Section 120.57(3), Florida Statutes, within ten (10) days of the date on which the written notice of protest is filed. At the time of filing the formal written protest, a bond (a cashier's check or money order may be accepted) payable to the Department must also be submitted in an amount equal to one percent (1%) of the estimated contract amount based on the contract price submitted by the protestor.

Failure to file a protest within the time prescribed in Section 120.57(3), Florida Statutes, or failure to post the bond or other security required by law within the time allowed for filing a bond shall constitute a waiver of proceedings under Chapter 120, Florida Statutes.

31.2 - Inability to Post:

If the Department is unable to post as defined above, the Department will notify all proposers by electronic notification on the Florida Vendor Bid System (see special condition 31.1, above) or by mail, fax, and/or telephone. The Department will provide notification of any future posting in a timely manner.

31.3 - Request to Withdraw Proposal:

Requests for withdrawal will be considered if received by the Department, in writing, within seventy-two (72) hours after the price proposal opening time and date. Requests received in accordance with this provision will be granted by the Department upon proof of the impossibility to perform based upon obvious error on the part of the proposer.

32) AWARD OF THE CONTRACT

Services will be authorized to begin when the Vendor receives the following document(s), as appropriate, indicating the encumbrance of funds and award of the contract:

- a) A Standard Written Agreement executed by both parties, and a written Notice to Proceed, issued by the Project Manager.

33) ATTACHMENTS

- Attachment A – Non-Disclosure Affidavit
- Attachment B – Payment Card Industry Data security Standard
- Attachment C – Visa Fraud Control and Investigations Procedures
- Attachment D – Certification Disbursement of Previous Payments
- Attachment E – Certificate of Completion

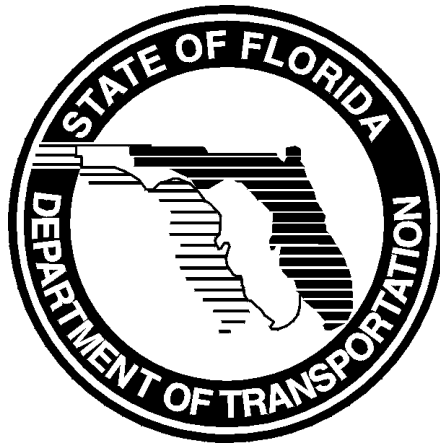
34) ATTACHED FORMS

- Form 1 – Certification of Experience Documentation (two pages)
- Form 2 – Drug-Free Workplace Program/ Vehicle Registration/Notice to Sublet Certification
- Form 3 - Asbestos Notification
- Form 4 - Corporate Resolution (If person signing for the firm is someone other than the Owner or President, a copy of the Corporate Resolution granting signature authorization must be furnished with the Technical Proposal.)

35) ATTACHED FORMS PUR 1000, GENERAL CONTRACT CONDITIONS AND PUR 1001, GENERAL INSTRUCTIONS TO REpondENTS

These are standard forms from the Department of Management Services that the Department is required to include in all formal solicitations. The following paragraphs do not apply to this Request for Proposal:

- Paragraph 3, Electronic Submission – PUR 1001
- Paragraph 4, Terms and Conditions – PUR1001
- Paragraph 5, Questions – PUR 1001
- Paragraph 31, Dispute Resolution - PUR 1000



PUR 1000 GENERAL CONTRACT CONDITIONS

RFP-DOT- 09/10-8001-KB

PAYMENT CARD INDUSTRY (PCI) SERVICES

FPI No. 423249-1-32-01

**State of Florida
PUR 1000
General Contract Conditions**

Contents

1. Definitions.
2. Purchase Orders.
3. Product Version.
4. Price Changes Applicable only to Term Contracts.
5. Additional Quantities.
6. Packaging.
7. Inspection at Contractor's Site.
8. Safety Standards.
9. Americans with Disabilities Act.
10. Literature.
11. Transportation and Delivery.
12. Installation.
13. Risk of Loss.
14. Transaction Fee.
15. Invoicing and Payment.
16. Taxes.
17. Governmental Restrictions.
18. Lobbying and Integrity.
19. Indemnification.
20. Limitation of Liability.
21. Suspension of Work.
22. Termination for Convenience.
23. Termination for Cause.
24. Force Majeure, Notice of Delay, and No Damages for Delay.
25. Changes.
26. Renewal.
27. Purchase Order Duration.
28. Advertising.
29. Assignment.
30. Antitrust Assignment
31. Dispute Resolution.
32. Employees, Subcontractors, and Agents.
33. Security and Confidentiality.
34. Contractor Employees, Subcontractors, and Other Agents.
35. Insurance Requirements.
36. Warranty of Authority.
37. Warranty of Ability to Perform.
38. Notices.
39. Leases and Installment Purchases.
40. Prison Rehabilitative Industries and Diversified Enterprises, Inc. (PRIDE).
41. Products Available from the Blind or Other Handicapped.
42. Modification of Terms.
43. Cooperative Purchasing.
44. Waiver.
45. Annual Appropriations.
46. Execution in Counterparts.
47. Severability.

1. Definitions. The definitions contained in s. 60A-1.001, F.A.C. shall apply to this agreement. The following additional terms are also defined:

(a) "Contract" means the legally enforceable agreement that results from a successful solicitation. The parties to the Contract will be the Customer and Contractor.

(b) "Customer" means the State agency or other entity identified in a contract as the party to receive commodities or contractual services pursuant to a contract or that orders commodities or contractual services via purchase order or other contractual instrument from the Contractor under the Contract. The "Customer" may also be the "Buyer" as defined in the PUR 1001 if it meets the definition of both terms.

(c) "Product" means any deliverable under the Contract, which may include commodities, services, technology or software.

(d) "Purchase order" means the form or format a Customer uses to make a purchase under the Contract (e.g., a formal written purchase order, electronic purchase order, procurement card, contract or other authorized means).

2. Purchase Orders. In contracts where commodities or services are ordered by the Customer via purchase order, Contractor shall not deliver or furnish products until a Customer transmits a purchase order. All purchase orders shall bear the Contract or solicitation number, shall be placed by the Customer directly with the Contractor, and shall be deemed to incorporate by reference the Contract and solicitation terms and conditions. Any discrepancy between the Contract terms and the terms stated on the Contractor's order form, confirmation, or acknowledgement shall be resolved in favor of terms most favorable to the Customer. A purchase order for services within the ambit of section 287.058(1) of the Florida Statutes shall be deemed to incorporate by reference the requirements of subparagraphs (a) through (f) thereof. Customers shall designate a contract manager and a contract administrator as required by subsections 287.057(15) and (16) of the Florida Statutes.

3. Product Version. Purchase orders shall be deemed to reference a manufacturer's most recently release model or version of the product at the time of the order, unless the Customer specifically requests in writing an earlier model or version and the contractor is willing to provide such model or version.

4. Price Changes Applicable only to Term Contracts. If this is a term contract for commodities or services, the following provisions apply.

(a) Quantity Discounts. Contractors are urged to offer additional discounts for one time delivery of large single orders. Customers should seek to negotiate additional price concessions on quantity purchases of any products offered under the Contract. State Customers shall document their files accordingly.

(b) Best Pricing Offer. During the Contract term, if the Customer becomes aware of better pricing offered by the Contractor for substantially the same or a smaller quantity of a product outside the Contract, but upon the same or similar terms of the Contract, then at the discretion of the Customer the price under the Contract shall be immediately reduced to the lower price.

(c) Sales Promotions. In addition to decreasing prices for the balance of the Contract term due to a change in market conditions, a Contractor may conduct sales promotions involving price reductions for a specified lesser period. A Contractor shall submit to the Contract Specialist documentation identifying the proposed (1) starting and ending dates of the promotion, (2) products involved, and (3) promotional prices compared to then-authorized prices. Promotional prices shall be available to all Customers. Upon approval, the Contractor shall provide conspicuous notice of the promotion.

(d) Trade-In. Customers may trade-in equipment when making purchases from the Contract. A trade-in shall be negotiated between the Customer and the Contractor. Customers are obligated to actively seek current fair market value when trading equipment, and to keep accurate records of the process. For State agencies, it may be necessary to provide documentation to the Department of Financial Services and to the agency property custodian pursuant to Chapter 273, F.S.

(e) Equitable Adjustment. The Customer may, in its sole discretion, make an equitable adjustment in the Contract terms or pricing if pricing or availability of supply is affected by extreme and unforeseen volatility in the marketplace, that is, by circumstances that satisfy all the following criteria: (1) the volatility is due to causes wholly beyond the Contractor's control, (2) the volatility affects the marketplace or industry, not just the particular Contract source of supply, (3) the

effect on pricing or availability of supply is substantial, and (4) the volatility so affects the Contractor that continued performance of the Contract would result in a substantial loss.

5. Additional Quantities. For a period not exceeding ninety (90) days from the date of solicitation award, the Customer reserves the right to acquire additional quantities up to the amount shown on the solicitation but not to exceed the threshold for Category Two at the prices submitted in the response to the solicitation.

6. Packaging. Tangible product shall be securely and properly packed for shipment, storage, and stocking in appropriate, clearly labeled, shipping containers and according to accepted commercial practice, without extra charge for packing materials, cases, or other types of containers. All containers and packaging shall become and remain Customer's property.

7. Inspection at Contractor's Site. The Customer reserves the right to inspect, at any reasonable time with prior notice, the equipment or product or plant or other facilities of a Contractor to assess conformity with Contract requirements and to determine whether they are adequate and suitable for proper and effective Contract performance.

8. Safety Standards. All manufactured items and fabricated assemblies subject to operation under pressure, operation by connection to an electric source, or operation involving connection to a manufactured, natural, or LP gas source shall be constructed and approved in a manner acceptable to the appropriate State inspector. Acceptability customarily requires, at a minimum, identification marking of the appropriate safety standard organization, where such approvals of listings have been established for the type of device offered and furnished, for example: the American Society of Mechanical Engineers for pressure vessels; the Underwriters Laboratories and/or National Electrical Manufacturers' Association for electrically operated assemblies; and the American Gas Association for gas-operated assemblies. In addition, all items furnished shall meet all applicable requirements of the Occupational Safety and Health Act and state and federal requirements relating to clean air and water pollution.

9. Americans with Disabilities Act. Contractors should identify any products that may be used or adapted for use by visually, hearing, or other physically impaired individuals.

10. Literature. Upon request, the Contractor shall furnish literature reasonably related to the product offered, for example, user manuals, price schedules, catalogs, descriptive brochures, etc.

11. Transportation and Delivery. Prices shall include all charges for packing, handling, freight, distribution, and inside delivery. Transportation of goods shall be FOB Destination to any point within thirty (30) days after the Customer places an Order. A Contractor, within five (5) days after receiving a purchase order, shall notify the Customer of any potential delivery delays. Evidence of inability or intentional delays shall be cause for Contract cancellation and Contractor suspension.

12. Installation. Where installation is required, Contractor shall be responsible for placing and installing the product in the required locations at no additional charge, unless otherwise designated on the Contract or purchase order. Contractor's authorized product and price list shall clearly and separately identify any additional installation charges. All materials used in the installation shall be of good quality and shall be free of defects that would diminish the appearance of the product or render it structurally or operationally unsound. Installation includes the furnishing of any equipment, rigging, and materials required to install or replace the product in the proper location. Contractor shall protect the site from damage and shall repair damages or injury caused during installation by Contractor or its employees or agents. If any alteration, dismantling, excavation, etc., is required to achieve installation, the Contractor shall promptly restore the structure or site to its original condition. Contractor shall perform installation work so as to cause the least inconvenience and interference with Customers and with proper consideration of others on site. Upon completion of the installation, the location and surrounding area of work shall be left

clean and in a neat and unobstructed condition, with everything in satisfactory repair and order.

13. Risk of Loss. Matters of inspection and acceptance are addressed in s. 215.422, F.S. Until acceptance, risk of loss or damage shall remain with the Contractor. The Contractor shall be responsible for filing, processing, and collecting all damage claims. To assist the Contractor with damage claims, the Customer shall: record any evidence of visible damage on all copies of the delivering carrier's Bill of Lading; report damages to the carrier and the Contractor; and provide the Contractor with a copy of the carrier's Bill of Lading and damage inspection report. When a Customer rejects a product, Contractor shall remove it from the premises within ten days after notification or rejection. Upon rejection notification, the risk of loss of rejected or non-conforming product shall remain with the Contractor. Rejected product not removed by the Contractor within ten days shall be deemed abandoned by the Contractor, and the Customer shall have the right to dispose of it as its own property. Contractor shall reimburse the Customer for costs and expenses incurred in storing or effecting removal or disposition of rejected product.

14. Transaction Fee. The State of Florida has instituted MyFloridaMarketPlace, a statewide eProcurement System ("System"). Pursuant to section 287.057(23), Florida Statutes (2002), all payments shall be assessed a Transaction Fee of one percent (1.0%), which the Contractor shall pay to the State, unless exempt pursuant to 60A-1.032, F.A.C.

For payments within the State accounting system (FLAIR or its successor), the Transaction Fee shall, when possible, be automatically deducted from payments to the Contractor. If automatic deduction is not possible, the Contractor shall pay the Transaction Fee pursuant to Rule 60A-1.031(2), F.A.C. By submission of these reports and corresponding payments, Contractor certifies their correctness. All such reports and payments shall be subject to audit by the State or its designee.

Contractor shall receive a credit for any Transaction Fee paid by the Contractor for the purchase of any item(s) if such item(s) are returned to the Contractor through no fault, act, or omission of the Contractor. Notwithstanding the foregoing, a Transaction Fee is non-refundable when an item is rejected or returned, or declined, due to the Contractor's failure to perform or comply with specifications or requirements of the agreement.

Failure to comply with these requirements shall constitute grounds for declaring the Contractor in default and recovering repurchase costs from the Contractor in addition to all outstanding fees. **CONTRACTORS DELINQUENT IN PAYING TRANSACTION FEES MAY BE SUBJECT TO BEING REMOVED FROM THE DEPARTMENT OF MANAGEMENT SERVICES' VENDOR LIST AS PROVIDED IN RULE 60A-1.006, F.A.C.**

15. Invoicing and Payment. Invoices shall contain the Contract number, purchase order number if applicable, and the appropriate vendor identification number. The State may require any other information from the Contractor that the State deems necessary to verify any purchase order placed under the Contract.

At the State's option, Contractors may be required to invoice electronically pursuant to guidelines of the Department of Management Services. Current guidelines require that Contractor supply electronic invoices in lieu of paper-based invoices for those transactions processed through the system. Electronic invoices shall be submitted to the Customer through the Ariba Supplier Network (ASN) in one of the following mechanisms - EDI 810, cXML, or web-based invoice entry within the ASN.

Payment shall be made in accordance with sections 215.422 and 287.0585 of the Florida Statutes, which govern time limits for payment of invoices. Invoices that must be returned to a Contractor due to preparation errors will result in a delay in payment. Contractors may call (850) 413-7269 Monday through Friday to inquire about the status of payments by State Agencies. The Customer is responsible for all payments under the Contract. A Customer's failure to pay, or delay in payment, shall not constitute a breach of the Contract and shall not relieve the Contractor of its obligations to the Department or to other Customers.

16. Taxes. The State does not pay Federal excise or sales taxes on direct purchases of tangible personal property. The State will not pay for any personal property taxes

levied on the Contractor or for any taxes levied on employees' wages. Any exceptions to this paragraph shall be explicitly noted by the Customer in the special contract conditions section of the solicitation or in the Contract or purchase order.

17. Governmental Restrictions. If the Contractor believes that any governmental restrictions have been imposed that require alteration of the material, quality, workmanship or performance of the products offered under the Contract, the Contractor shall immediately notify the Customer in writing, indicating the specific restriction. The Customer reserves the right and the complete discretion to accept any such alteration or to cancel the Contract at no further expense to the Customer.

18. Lobbying and Integrity. Customers shall ensure compliance with Section 11.062, FS and Section 216.347, FS. The Contractor shall not, in connection with this or any other agreement with the State, directly or indirectly (1) offer, confer, or agree to confer any pecuniary benefit on anyone as consideration for any State officer or employee's decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty, or (2) offer, give, or agree to give to anyone any gratuity for the benefit of, or at the direction or request of, any State officer or employee. For purposes of clause (2), "gratuity" means any payment of more than nominal monetary value in the form of cash, travel, entertainment, gifts, meals, lodging, loans, subscriptions, advances, deposits of money, services, employment, or contracts of any kind. Upon request of the Customer's Inspector General, or other authorized State official, the Contractor shall provide any type of information the Inspector General deems relevant to the Contractor's integrity or responsibility. Such information may include, but shall not be limited to, the Contractor's business or financial records, documents, or files of any type or form that refer to or relate to the Contract. The Contractor shall retain such records for the longer of (1) three years after the expiration of the Contract or (2) the period required by the General Records Schedules maintained by the Florida Department of State (available at: <http://dlis.dos.state.fl.us/barm/genschedules/gensched.htm>). The Contractor agrees to reimburse the State for the reasonable costs of investigation incurred by the Inspector General or other authorized State official for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the State which results in the suspension or debarment of the Contractor. Such costs shall include, but shall not be limited to: salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees. The Contractor shall not be responsible for any costs of investigations that do not result in the Contractor's suspension or debarment.

19. Indemnification. The Contractor shall be fully liable for the actions of its agents, employees, partners, or subcontractors and shall fully indemnify, defend, and hold harmless the State and Customers, and their officers, agents, and employees, from suits, actions, damages, and costs of every name and description, including attorneys' fees, arising from or relating to personal injury and damage to real or personal tangible property alleged to be caused in whole or in part by Contractor, its agents, employees, partners, or subcontractors, provided, however, that the Contractor shall not indemnify for that portion of any loss or damages proximately caused by the negligent act or omission of the State or a Customer.

Further, the Contractor shall fully indemnify, defend, and hold harmless the State and Customers from any suits, actions, damages, and costs of every name and description, including attorneys' fees, arising from or relating to violation or infringement of a trademark, copyright, patent, trade secret or intellectual property right, provided, however, that the foregoing obligation shall not apply to a Customer's misuse or modification of Contractor's products or a Customer's operation or use of Contractor's products in a manner not contemplated by the Contract or the purchase order. If any product is the subject of an infringement suit, or in the Contractor's opinion is likely to become the subject of such a suit, the Contractor may at its sole expense procure for the Customer the right to continue using the product or to modify it to become non-infringing. If the Contractor is not reasonably able to modify or otherwise secure the Customer the right to continue using the product, the Contractor shall remove the product and refund the Customer the amounts paid in excess of a reasonable rental for past use. The customer shall not be liable for any royalties.

The Contractor's obligations under the preceding two paragraphs with respect to any legal action are contingent upon the State or Customer giving the Contractor (1) written notice of any action or threatened action, (2) the opportunity to take over and settle

or defend any such action at Contractor's sole expense, and (3) assistance in defending the action at Contractor's sole expense. The Contractor shall not be liable for any cost, expense, or compromise incurred or made by the State or Customer in any legal action without the Contractor's prior written consent, which shall not be unreasonably withheld.

20. Limitation of Liability. For all claims against the Contractor under any contract or purchase order, and regardless of the basis on which the claim is made, the Contractor's liability under a contract or purchase order for direct damages shall be limited to the greater of \$100,000, the dollar amount of the contract or purchase order, or two times the charges rendered by the Contractor under the purchase order. This limitation shall not apply to claims arising under the Indemnity paragraph contain in this agreement.

Unless otherwise specifically enumerated in the Contract or in the purchase order, no party shall be liable to another for special, indirect, punitive, or consequential damages, including lost data or records (unless the contract or purchase order requires the Contractor to back-up data or records), even if the party has been advised that such damages are possible. No party shall be liable for lost profits, lost revenue, or lost institutional operating savings. The State and Customer may, in addition to other remedies available to them at law or equity and upon notice to the Contractor, retain such monies from amounts due Contractor as may be necessary to satisfy any claim for damages, penalties, costs and the like asserted by or against them. The State may set off any liability or other obligation of the Contractor or its affiliates to the State against any payments due the Contractor under any contract with the State.

21. Suspension of Work. The Customer may in its sole discretion suspend any or all activities under the Contract or purchase order, at anytime, when in the best interests of the State to do so. The Customer shall provide the Contractor written notice outlining the particulars of suspension. Examples of the reason for suspension include, but are not limited to, budgetary constraints, declaration of emergency, or other such circumstances. After receiving a suspension notice, the Contractor shall comply with the notice and shall not accept any purchase orders. Within ninety days, or any longer period agreed to by the Contractor, the Customer shall either (1) issue a notice authorizing resumption of work, at which time activity shall resume, or (2) terminate the Contract or purchase order. Suspension of work shall not entitle the Contractor to any additional compensation.

22. Termination for Convenience. The Customer, by written notice to the Contractor, may terminate the Contract in whole or in part when the Customer determines in its sole discretion that it is in the State's interest to do so. The Contractor shall not furnish any product after it receives the notice of termination, except as necessary to complete the continued portion of the Contract, if any. The Contractor shall not be entitled to recover any cancellation charges or lost profits.

23. Termination for Cause. The Customer may terminate the Contract if the Contractor fails to (1) deliver the product within the time specified in the Contract or any extension, (2) maintain adequate progress, thus endangering performance of the Contract, (3) honor any term of the Contract, or (4) abide by any statutory, regulatory, or licensing requirement. Rule 60A-1.006(3), F.A.C., governs the procedure and consequences of default. The Contractor shall continue work on any work not terminated. Except for defaults of subcontractors at any tier, the Contractor shall not be liable for any excess costs if the failure to perform the Contract arises from events completely beyond the control, and without the fault or negligence, of the Contractor. If the failure to perform is caused by the default of a subcontractor at any tier, and if the cause of the default is completely beyond the control of both the Contractor and the subcontractor, and without the fault or negligence of either, the Contractor shall not be liable for any excess costs for failure to perform, unless the subcontracted products were obtainable from other sources in sufficient time for the Contractor to meet the required delivery schedule. If, after termination, it is determined that the Contractor was not in default, or that the default was excusable, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of the Customer. The rights and remedies of the Customer in this clause are in addition to any other rights and remedies provided by law or under the Contract.

24. Force Majeure, Notice of Delay, and No Damages for Delay. The Contractor shall not be responsible for delay resulting from its failure to perform if neither the fault nor the

negligence of the Contractor or its employees or agents contributed to the delay and the delay is due directly to acts of God, wars, acts of public enemies, strikes, fires, floods, or other similar cause wholly beyond the Contractor's control, or for any of the foregoing that affect subcontractors or suppliers if no alternate source of supply is available to the Contractor. In case of any delay the Contractor believes is excusable, the Contractor shall notify the Customer in writing of the delay or potential delay and describe the cause of the delay either (1) within ten (10) days after the cause that creates or will create the delay first arose, if the Contractor could reasonably foresee that a delay could occur as a result, or (2) if delay is not reasonably foreseeable, within five (5) days after the date the Contractor first had reason to believe that a delay could result. **THE FOREGOING SHALL CONSTITUTE THE CONTRACTOR'S SOLE REMEDY OR EXCUSE WITH RESPECT TO DELAY.** Providing notice in strict accordance with this paragraph is a condition precedent to such remedy. No claim for damages, other than for an extension of time, shall be asserted against the Customer. The Contractor shall not be entitled to an increase in the Contract price or payment of any kind from the Customer for direct, indirect, consequential, impact or other costs, expenses or damages, including but not limited to costs of acceleration or inefficiency, arising because of delay, disruption, interference, or hindrance from any cause whatsoever. If performance is suspended or delayed, in whole or in part, due to any of the causes described in this paragraph, after the causes have ceased to exist the Contractor shall perform at no increased cost, unless the Customer determines, in its sole discretion, that the delay will significantly impair the value of the Contract to the State or to Customers, in which case the Customer may (1) accept allocated performance or deliveries from the Contractor, provided that the Contractor grants preferential treatment to Customers with respect to products subjected to allocation, or (2) purchase from other sources (without recourse to and by the Contractor for the related costs and expenses) to replace all or part of the products that are the subject of the delay, which purchases may be deducted from the Contract quantity, or (3) terminate the Contract in whole or in part.

25. Changes. The Customer may unilaterally require, by written order, changes altering, adding to, or deducting from the Contract specifications, provided that such changes are within the general scope of the Contract. The Customer may make an equitable adjustment in the Contract price or delivery date if the change affects the cost or time of performance. Such equitable adjustments require the written consent of the Contractor, which shall not be unreasonably withheld. If unusual quantity requirements arise, the Customer may solicit separate bids to satisfy them.

26. Renewal. Upon mutual agreement, the Customer and the Contractor may renew the Contract, in whole or in part, for a period that may not exceed 3 years or the term of the contract, whichever period is longer. Any renewal shall specify the renewal price, as set forth in the solicitation response. The renewal must be in writing and signed by both parties, and is contingent upon satisfactory performance evaluations and subject to availability of funds.

27. Purchase Order Duration. Purchase orders issued pursuant to a state term or agency contract must be received by the Contractor no later than close of business on the last day of the contract's term to be considered timely. The Contractor is obliged to fill those orders in accordance with the contract's terms and conditions. Purchase orders received by the contractor after close of business on the last day of the state term or agency contract's term shall be considered void.

Purchase orders for a one-time delivery of commodities or performance of contractual services shall be valid through the performance by the Contractor, and all terms and conditions of the state term or agency contract shall apply to the single delivery/performance, and shall survive the termination of the Contract.

Contractors are required to accept purchase orders specifying delivery schedules exceeding the contracted schedule even when such extended delivery will occur after expiration of the state term or agency contract. For example, if a state term contract calls for delivery 30 days after receipt of order (ARO), and an order specifies delivery will occur both in excess of 30 days ARO and after expiration of the state term contract, the Contractor will accept the order. However, if the Contractor expressly and in writing notifies the ordering office within ten (10) calendar days of receipt of the purchase order that Contractor will not accept the extended delivery terms beyond the expiration of the state term contract, then the purchase order will either be amended in writing by the ordering entity within ten (10) calendar days of receipt of the contractor's notice to reflect the state term contract delivery schedule, or it

shall be considered withdrawn.

The duration of purchase orders for recurring deliveries of commodities or performance of services shall not exceed the expiration of the state term or agency contract by more than twelve months. However, if an extended pricing plan offered in the state term or agency contract is selected by the ordering entity, the contract terms on pricing plans and renewals shall govern the maximum duration of purchase orders reflecting such pricing plans and renewals.

Timely purchase orders shall be valid through their specified term and performance by the Contractor, and all terms and conditions of the state term or agency contract shall apply to the recurring delivery/performance as provided herein, and shall survive the termination of the Contract.

Ordering offices shall not renew a purchase order issued pursuant to a state term or agency contract if the underlying contract expires prior to the effective date of the renewal.

28. Advertising. Subject to Chapter 119, Florida Statutes, the Contractor shall not publicly disseminate any information concerning the Contract without prior written approval from the Customer, including, but not limited to mentioning the Contract in a press release or other promotional material, identifying the Customer or the State as a reference, or otherwise linking the Contractor's name and either a description of the Contract or the name of the State or the Customer in any material published, either in print or electronically, to any entity that is not a party to Contract, except potential or actual authorized distributors, dealers, resellers, or service representative.

29. Assignment. The Contractor shall not sell, assign or transfer any of its rights, duties or obligations under the Contract, or under any purchase order issued pursuant to the Contract, without the prior written consent of the Customer. In the event of any assignment, the Contractor remains secondarily liable for performance of the contract, unless the Customer expressly waives such secondary liability. The Customer may assign the Contract with prior written notice to Contractor of its intent to do so.

30. Antitrust Assignment. The Contractor and the State of Florida recognize that in actual economic practice, overcharges resulting from antitrust violations are in fact usually borne by the State of Florida. Therefore, the contractor hereby assigns to the State of Florida any and all claims for such overcharges as to goods, materials or services purchased in connection with the Contract.

31. Dispute Resolution. Any dispute concerning performance of the Contract shall be decided by the Customer's designated contract manager, who shall reduce the decision to writing and serve a copy on the Contractor. The decision shall be final and conclusive unless within twenty one (21) days from the date of receipt, the Contractor files with the Customer a petition for administrative hearing. The Customer's decision on the petition shall be final, subject to the Contractor's right to review pursuant to Chapter 120 of the Florida Statutes. Exhaustion of administrative remedies is an absolute condition precedent to the Contractor's ability to pursue any other form of dispute resolution; provided, however, that the parties may employ the alternative dispute resolution procedures outlined in Chapter 120.

Without limiting the foregoing, the exclusive venue of any legal or equitable action that arises out of or relates to the Contract shall be the appropriate state court in Leon County, Florida; in any such action, Florida law shall apply and the parties waive any right to jury trial.

32. Employees, Subcontractors, and Agents. All Contractor employees, subcontractors, or agents performing work under the Contract shall be properly trained technicians who meet or exceed any specified training qualifications. Upon request, Contractor shall furnish a copy of technical certification or other proof of qualification. All employees, subcontractors, or agents performing work under the Contract must comply with all security and administrative requirements of the Customer and shall comply with all controlling laws and regulations relevant to the services they are providing under the Contract. The State may conduct, and the Contractor shall cooperate in, a security background check or otherwise assess any employee, subcontractor, or agent furnished by the Contractor. The State may refuse access to, or require replacement of, any

personnel for cause, including, but not limited to, technical or training qualifications, quality of work, change in security status, or non-compliance with a Customer's security or other requirements. Such approval shall not relieve the Contractor of its obligation to perform all work in compliance with the Contract. The State may reject and bar from any facility for cause any of the Contractor's employees, subcontractors, or agents.

33. Security and Confidentiality. The Contractor shall comply fully with all security procedures of the United States, State of Florida and Customer in performance of the Contract. The Contractor shall not divulge to third parties any confidential information obtained by the Contractor or its agents, distributors, resellers, subcontractors, officers or employees in the course of performing Contract work, including, but not limited to, security procedures, business operations information, or commercial proprietary information in the possession of the State or Customer. The Contractor shall not be required to keep confidential information or material that is publicly available through no fault of the Contractor, material that the Contractor developed independently without relying on the State's or Customer's confidential information, or material that is otherwise obtainable under State law as a public record. To insure confidentiality, the Contractor shall take appropriate steps as to its personnel, agents, and subcontractors. The warranties of this paragraph shall survive the Contract.

34. Contractor Employees, Subcontractors, and Other Agents. The Customer and the State shall take all actions necessary to ensure that Contractor's employees, subcontractors and other agents are not employees of the State of Florida. Such actions include, but are not limited to, ensuring that Contractor's employees, subcontractors, and other agents receive benefits and necessary insurance (health, workers' compensations, and unemployment) from an employer other than the State of Florida.

35. Insurance Requirements. During the Contract term, the Contractor at its sole expense shall provide commercial insurance of such a type and with such terms and limits as may be reasonably associated with the Contract. Providing and maintaining adequate insurance coverage is a material obligation of the Contractor. Upon request, the Contractor shall provide certificate of insurance. The limits of coverage under each policy maintained by the Contractor shall not be interpreted as limiting the Contractor's liability and obligations under the Contract. All insurance policies shall be through insurers authorized or eligible to write policies in Florida.

36. Warranty of Authority. Each person signing the Contract warrants that he or she is duly authorized to do so and to bind the respective party to the Contract.

37. Warranty of Ability to Perform. The Contractor warrants that, to the best of its knowledge, there is no pending or threatened action, proceeding, or investigation, or any other legal or financial condition, that would in any way prohibit, restrain, or diminish the Contractor's ability to satisfy its Contract obligations. The Contractor warrants that neither it nor any affiliate is currently on the convicted vendor list maintained pursuant to section 287.133 of the Florida Statutes, or on any similar list maintained by any other state or the federal government. The Contractor shall immediately notify the Customer in writing if its ability to perform is compromised in any manner during the term of the Contract.

38. Notices. All notices required under the Contract shall be delivered by certified mail, return receipt requested, by reputable air courier service, or by personal delivery to the agency designee identified in the original solicitation, or as otherwise identified by the Customer. Notices to the Contractor shall be delivered to the person who signs the Contract. Either designated recipient may notify the other, in writing, if someone else is designated to receive notice.

39. Leases and Installment Purchases. Prior approval of the Chief Financial Officer (as defined in Section 17.001, F.S.) is required for State agencies to enter into or to extend any lease or installment-purchase agreement in excess of the Category Two amount established by section 287.017 of the Florida Statutes.

40. Prison Rehabilitative Industries and Diversified Enterprises, Inc. (PRIDE). Section 946.515(2), F.S. requires the following statement to be included in the solicitation: "It is expressly understood and agreed that any articles which are the subject of, or required to carry out, the Contract shall be purchased from the corporation identified under

Chapter 946 of the Florida Statutes (PRIDE) in the same manner and under the same procedures set forth in section 946.515(2) and (4) of the Florida Statutes; and for purposes of the Contract the person, firm, or other business entity carrying out the provisions of the Contract shall be deemed to be substituted for the agency insofar as dealings with such corporation are concerned." Additional information about PRIDE and the products it offers is available at <http://www.pridefl.com>.

41. Products Available from the Blind or Other Handicapped. Section 413.036(3), F.S. requires the following statement to be included in the solicitation: "It is expressly understood and agreed that any articles that are the subject of, or required to carry out, this contract shall be purchased from a nonprofit agency for the Blind or for the Severely Handicapped that is qualified pursuant to Chapter 413, Florida Statutes, in the same manner and under the same procedures set forth in section 413.036(1) and (2), Florida Statutes; and for purposes of this contract the person, firm, or other business entity carrying out the provisions of this contract shall be deemed to be substituted for the State agency insofar as dealings with such qualified nonprofit agency are concerned." Additional information about the designated nonprofit agency and the products it offers is available at <http://www.respectofflorida.org>.

42. Modification of Terms. The Contract contains all the terms and conditions agreed upon by the parties, which terms and conditions shall govern all transactions between the Customer and the Contractor. The Contract may only be modified or amended upon mutual written agreement of the Customer and the Contractor. No oral agreements or representations shall be valid or binding upon the Customer or the Contractor. No alteration or modification of the Contract terms, including substitution of product, shall be valid or binding against the Customer. The Contractor may not unilaterally modify the terms of the Contract by affixing additional terms to product upon delivery (e.g., attachment or inclusion of standard preprinted forms, product literature, "shrink wrap" terms accompanying or affixed to a product, whether written or electronic) or by incorporating such terms onto the Contractor's order or fiscal forms or other documents forwarded by the Contractor for payment. The Customer's acceptance of product or processing of documentation on forms furnished by the Contractor for approval or payment shall not constitute acceptance of the proposed modification to terms and conditions.

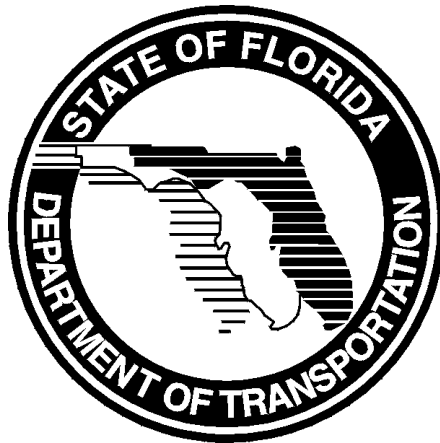
43. Cooperative Purchasing. Pursuant to their own governing laws, and subject to the agreement of the Contractor, other entities may be permitted to make purchases at the terms and conditions contained herein. Non-Customer purchases are independent of the agreement between Customer and Contractor, and Customer shall not be a party to any transaction between the Contractor and any other purchaser. State agencies wishing to make purchases from this agreement are required to follow the provisions of s. 287.042(16)(a), F.S. This statute requires the Department of Management Services to determine that the requestor's use of the contract is cost-effective and in the best interest of the State.

44. Waiver. The delay or failure by the Customer to exercise or enforce any of its rights under this Contract shall not constitute or be deemed a waiver of the Customer's right thereafter to enforce those rights, nor shall any single or partial exercise of any such right preclude any other or further exercise thereof or the exercise of any other right.

45. Annual Appropriations. The State's performance and obligation to pay under this contract are contingent upon an annual appropriation by the Legislature.

46. Execution in Counterparts. The Contract may be executed in counterparts, each of which shall be an original and all of which shall constitute but one and the same instrument.

47. Severability. If a court deems any provision of the Contract void or unenforceable, that provision shall be enforced only to the extent that it is not in violation of law or is not otherwise unenforceable and all other provisions shall remain in full force and effect.



PUR 1001 GENERAL INSTRUCTIONS TO RESPONDENTS

RFP-DOT- 09/10-8001-KB

PAYMENT CARD INDUSTRY (PCI) SERVICES

FPI No. 423249-1-32-01

**State of Florida
PUR 1001
General Instructions to Respondents**

Contents

1. Definitions.
2. General Instructions.
3. Electronic Submission of Responses.
4. Terms and Conditions.
5. Questions.
6. Conflict of Interest.
7. Convicted Vendors.
8. Discriminatory Vendors.
9. Respondent's Representation and Authorization.
- [10. Manufacturer's Name and Approved Equivalents.](#)
11. Performance Qualifications.
12. Public Opening.
13. Electronic Posting of Notice of Intended Award.
14. Firm Response.
15. Clarifications/Revisions.
16. Minor Irregularities/Right to Reject.
17. Contract Formation.
18. Contract Overlap.
19. Public Records.
20. Protests.
21. Limitation on Vendor Contact with Agency During Solicitation Period

1. Definitions. The definitions found in s. 60A-1.001, F.A.C. shall apply to this agreement. The following additional terms are also defined:

- (a) "Buyer" means the entity that has released the solicitation. The "Buyer" may also be the "Customer" as defined in the PUR 1000 if that entity meets the definition of both terms.
- (b) "Procurement Officer" means the Buyer's contracting personnel, as identified in the Introductory Materials.
- (c) "Respondent" means the entity that submits materials to the Buyer in accordance with these Instructions.
- (d) "Response" means the material submitted by the respondent in answering the solicitation.
- (e) "Timeline" means the list of critical dates and actions included in the Introductory Materials.

2. General Instructions. Potential respondents to the solicitation are encouraged to carefully review all the materials contained herein and prepare responses accordingly.

3. Electronic Submission of Responses. Respondents are required to submit responses electronically. For this purpose, all references herein to signatures, signing requirements, or other required acknowledgments hereby include electronic signature by means of clicking the "Submit Response" button (or other similar symbol or process) attached to or logically associated with the response created by the respondent within MyFloridaMarketPlace. The respondent agrees that the action of electronically submitting its response constitutes:

- an electronic signature on the response, generally,
- an electronic signature on any form or section specifically calling for a signature, and
- an affirmative agreement to any statement contained in the solicitation that requires a definite confirmation or acknowledgement.

4. Terms and Conditions. All responses are subject to the terms of the following sections of this solicitation, which, in case of conflict, shall have the order of precedence listed:

- Technical Specifications,
- Special Conditions and Instructions,
- Instructions to Respondents (PUR 1001),
- General Conditions (PUR 1000), and
- Introductory Materials.

The Buyer objects to and shall not consider any additional terms or conditions submitted by a respondent, including any appearing in documents attached as part of a respondent's response. In submitting its response, a respondent agrees that any additional terms or conditions, whether submitted intentionally or inadvertently, shall have no force or effect. Failure to comply with terms and conditions, including those specifying information that must be submitted with a response, shall be grounds for rejecting a response.

5. Questions. Respondents shall address all questions regarding this solicitation to the Procurement Officer. Questions must be submitted via the Q&A Board within MyFloridaMarketPlace and must be RECEIVED NO LATER THAN the time and date reflected on the Timeline. Questions shall be answered in accordance with the Timeline. All questions submitted shall be published and answered in a manner that all respondents will be able to view. Respondents shall not contact any other employee of the Buyer or the State for information with respect to this solicitation. Each respondent is responsible for monitoring the MyFloridaMarketPlace site for new or changing information. The Buyer shall not be bound by any verbal information or by any written information that is not contained within the solicitation documents or formally noticed and issued by the Buyer's contracting personnel. Questions to the Procurement Officer or to any Buyer personnel shall not constitute formal protest of the specifications or of the solicitation, a process addressed in paragraph 19 of these Instructions.

6. Conflict of Interest. This solicitation is subject to chapter 112 of the Florida Statutes. Respondents shall disclose with their response the name of any officer, director, employee or other agent who is also an employee of the State. Respondents shall also disclose the name of any State employee who owns, directly or indirectly, an interest of five percent (5%) or more in the respondent or its affiliates.

7. Convicted Vendors. A person or affiliate placed on the convicted vendor list following a conviction for a public entity crime is prohibited from doing any of the following for a period of 36 months from the date of being placed on the convicted vendor list:

- submitting a bid on a contract to provide any goods or services to a public entity;
- submitting a bid on a contract with a public entity for the construction or repair of a public building or public work;
- submitting bids on leases of real property to a public entity;
- being awarded or performing work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity; and
- transacting business with any public entity in excess of the Category Two threshold amount (\$25,000) provided in section 287.017 of the Florida Statutes.

8. Discriminatory Vendors. An entity or affiliate placed on the discriminatory vendor list pursuant to section 287.134 of the Florida Statutes may not:

- submit a bid on a contract to provide any goods or services to a public entity;
- submit a bid on a contract with a public entity for the construction or repair of a public building or public work;
- submit bids on leases of real property to a public entity;
- be awarded or perform work as a contractor, supplier, sub-contractor, or consultant under a contract with any public entity; or
- transact business with any public entity.

9. Respondent's Representation and Authorization. In submitting a response, each respondent

understands, represents, and acknowledges the following (if the respondent cannot so certify to any of following, the respondent shall submit with its response a written explanation of why it cannot do so).

- The respondent is not currently under suspension or debarment by the State or any other governmental authority.
- To the best of the knowledge of the person signing the response, the respondent, its affiliates, subsidiaries, directors, officers, and employees are not currently under investigation by any governmental authority and have not in the last ten (10) years been convicted or found liable for any act prohibited by law in any jurisdiction, involving conspiracy or collusion with respect to bidding on any public contract.
- Respondent currently has no delinquent obligations to the State, including a claim by the State for liquidated damages under any other contract.
- The submission is made in good faith and not pursuant to any agreement or discussion with, or inducement from, any firm or person to submit a complementary or other noncompetitive response.
- The prices and amounts have been arrived at independently and without consultation, communication, or agreement with any other respondent or potential respondent; neither the prices nor amounts, actual or approximate, have been disclosed to any respondent or potential respondent, and they will not be disclosed before the solicitation opening.
- The respondent has fully informed the Buyer in writing of all convictions of the firm, its affiliates (as defined in section 287.133(1)(a) of the Florida Statutes), and all directors, officers, and employees of the firm and its affiliates for violation of state or federal antitrust laws with respect to a public contract for violation of any state or federal law involving fraud, bribery, collusion, conspiracy or material misrepresentation with respect to a public contract. This includes disclosure of the names of current employees who were convicted of contract crimes while in the employ of another company.
- Neither the respondent nor any person associated with it in the capacity of owner, partner, director, officer, principal, investigator, project director, manager, auditor, or position involving the administration of federal funds:
 - o Has within the preceding three years been convicted of or had a civil judgment rendered against them or is presently indicted for or otherwise criminally or civilly charged for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a federal, state, or local government transaction or public contract; violation of federal or state antitrust statutes; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property; or
 - o Has within a three-year period preceding this certification had one or more federal, state, or local government contracts terminated for cause or default.
- The product offered by the respondent will conform to the specifications without exception.
- The respondent has read and understands the Contract terms and conditions, and the submission is made in conformance with those terms and conditions.
- If an award is made to the respondent, the respondent agrees that it intends to be legally bound to the Contract that is formed with the State.
- The respondent has made a diligent inquiry of its employees and agents responsible for preparing, approving, or submitting the response, and has been advised by each of them that he or she has not participated in any communication, consultation, discussion, agreement, collusion, act or other conduct inconsistent with any of the statements and representations made in the response.
- The respondent shall indemnify, defend, and hold harmless the Buyer and its employees against any cost, damage, or expense which may be incurred or be caused by any error in the respondent's preparation of its bid.
- All information provided by, and representations made by, the respondent are material and important and will be relied upon by the Buyer in awarding the Contract. Any misstatement shall be treated as fraudulent concealment from the Buyer of the true facts relating to submission of the bid. A misrepresentation shall be punishable under law, including, but not limited to, Chapter 817 of the Florida Statutes.

10. Manufacturer's Name and Approved Equivalents. Unless otherwise specified, any

manufacturers' names, trade names, brand names, information or catalog numbers listed in a specification are descriptive, not restrictive. With the Buyer's prior approval, the Contractor may provide any product that meets or exceeds the applicable specifications. The Contractor shall demonstrate comparability, including appropriate catalog materials, literature, specifications, test data, etc. The Buyer shall determine in its sole discretion whether a product is acceptable as an equivalent.

11. Performance Qualifications. The Buyer reserves the right to investigate or inspect at any time whether the product, qualifications, or facilities offered by Respondent meet the Contract requirements. Respondent shall at all times during the Contract term remain responsive and responsible. In determining Respondent's responsibility as a vendor, the agency shall consider all information or evidence which is gathered or comes to the attention of the agency which demonstrates the Respondent's capability to fully satisfy the requirements of the solicitation and the contract.

Respondent must be prepared, if requested by the Buyer, to present evidence of experience, ability, and financial standing, as well as a statement as to plant, machinery, and capacity of the respondent for the production, distribution, and servicing of the product bid. If the Buyer determines that the conditions of the solicitation documents are not complied with, or that the product proposed to be furnished does not meet the specified requirements, or that the qualifications, financial standing, or facilities are not satisfactory, or that performance is untimely, the Buyer may reject the response or terminate the Contract. Respondent may be disqualified from receiving awards if respondent, or anyone in respondent's employment, has previously failed to perform satisfactorily in connection with public bidding or contracts. This paragraph shall not mean or imply that it is obligatory upon the Buyer to make an investigation either before or after award of the Contract, but should the Buyer elect to do so, respondent is not relieved from fulfilling all Contract requirements.

12. Public Opening. Responses shall be opened on the date and at the location indicated on the Timeline. Respondents may, but are not required to, attend. The Buyer may choose not to announce prices or release other materials pursuant to s. 119.071(1)(b), Florida Statutes. Any person requiring a special accommodation because of a disability should contact the Procurement Officer at least five (5) workdays prior to the solicitation opening. If you are hearing or speech impaired, please contact the Buyer by using the Florida Relay Service at (800) 955-8771 (TDD).

13. Electronic Posting of Notice of Intended Award. Based on the evaluation, on the date indicated on the Timeline the Buyer shall electronically post a notice of intended award at http://fcn.state.fl.us/owa_vbs/owa/vbs/www.main.menu. If the notice of award is delayed, in lieu of posting the notice of intended award the Buyer shall post a notice of the delay and a revised date for posting the notice of intended award. Any person who is adversely affected by the decision shall file with the Buyer a notice of protest within 72 hours after the electronic posting. The Buyer shall not provide tabulations or notices of award by telephone.

14. Firm Response. The Buyer may make an award within sixty (60) days after the date of the opening, during which period responses shall remain firm and shall not be withdrawn. If award is not made within sixty (60) days, the response shall remain firm until either the Buyer awards the Contract or the Buyer receives from the respondent written notice that the response is withdrawn. Any response that expresses a shorter duration may, in the Buyer's sole discretion, be accepted or rejected.

15. Clarifications/Revisions. Before award, the Buyer reserves the right to seek clarifications or request any information deemed necessary for proper evaluation of submissions from all respondents deemed eligible for Contract award. Failure to provide requested information may result in rejection of the response.

16. Minor Irregularities/Right to Reject. The Buyer reserves the right to accept or reject any and all bids, or separable portions thereof, and to waive any minor irregularity, technicality, or omission if the Buyer determines that doing so will serve the State's best interests. The Buyer may reject any response not submitted in the manner specified by the solicitation documents.

17. Contract Formation. The Buyer shall issue a notice of award, if any, to successful respondent(s), however, no contract shall be formed between respondent and the Buyer until the Buyer signs the Contract. The Buyer shall not be liable for any costs incurred by a respondent in preparing or producing its response or for any work performed before the Contract is effective.

18. Contract Overlap. Respondents shall identify any products covered by this solicitation that they are currently authorized to furnish under any state term contract. By entering into the Contract, a Contractor authorizes the Buyer to eliminate duplication between agreements in the manner the Buyer deems to be in its best interest.

19. Public Records. Article 1, section 24, Florida Constitution, guarantees every person access to all public records, and Section 119.011, Florida Statutes, provides a broad definition of public record. As such, all responses to a competitive solicitation are public records unless exempt by law. Any respondent claiming that its response contains information that is exempt from the public records law shall clearly segregate and mark that information and provide the specific statutory citation for such exemption.

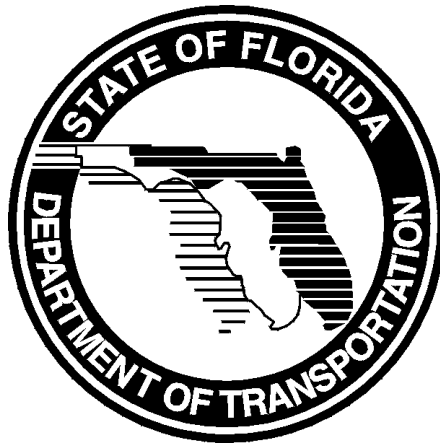
20. Protests. Any protest concerning this solicitation shall be made in accordance with sections 120.57(3) and 287.042(2) of the Florida Statutes and chapter 28-110 of the Florida Administrative Code. Questions to the Procurement Officer shall not constitute formal notice of a protest. It is the Buyer's intent to ensure that specifications are written to obtain the best value for the State and that specifications are written to ensure competitiveness, fairness, necessity and reasonableness in the solicitation process.

Section 120.57(3)(b), F.S. and Section 28-110.003, Fla. Admin. Code require that a notice of protest of the solicitation documents shall be made within seventy-two hours after the posting of the solicitation.

Section 120.57(3)(a), F.S. requires the following statement to be included in the solicitation: "Failure to file a protest within the time prescribed in section 120.57(3), Florida Statutes, shall constitute a waiver of proceedings under Chapter 120, Florida Statutes."

Section 28-110.005, Fla. Admin. Code requires the following statement to be included in the solicitation: "Failure to file a protest within the time prescribed in Section 120.57(3), Florida Statutes, or failure to post the bond or other security required by law within the time allowed for filing a bond shall constitute a waiver of proceedings under Chapter 120, Florida Statutes."

21. Limitation on Vendor Contact with Agency During Solicitation Period. Respondents to this solicitation or persons acting on their behalf may not contact, between the release of the solicitation and the end of the 72-hour period following the agency posting the notice of intended award, excluding Saturdays, Sundays, and state holidays, any employee or officer of the executive or legislative branch concerning any aspect of this solicitation, except in writing to the procurement officer or as provided in the solicitation documents. Violation of this provision may be grounds for rejecting a response.



FORMS

RFP-DOT- 09/10-8001-KB

PAYMENT CARD INDUSTRY (PCI) SERVICES

FPI No. 423249-1-32-01

CERTIFICATION OF EXPERIENCE DOCUMENTATION

I, _____, _____, of
(Print/Type Name) (Title)

_____, hereby certify that this Company has been in
(Name of Business)

business for a minimum of 5 years and has the experience to perform the services requested by RFP-DOT-09/10-8001-KB.

As I have indicated experience above, I now submit the following list of business and client references that will attest to our services and business relationships for the periods indicated and I hereby give permission to the Turnpike Enterprise to inquire for references as to my performance.

Signature: _____ Date: _____

Name Business: _____

Note: Describe your work experience in detail for the minimum period required, beginning with your current or most recent project. Use a separate block to describe each project. (Attach additional sheets as necessary.)

Date: (Mo. & Yr.): From _____ To _____ Dollar Value of Project: \$_____

Client Name: _____ Client's Project Manager: _____

Address: _____ City: _____

State: _____ Zip: _____ Phone: () _____ - _____ Fax: () _____ - _____

Project Description: _____

Date: (Mo. & Yr.): From _____ To _____ Dollar Value of Project: \$_____

Client Name: _____ Client's Project Manager: _____

Address: _____ City: _____

State: _____ Zip: _____ Phone: () _____ - _____ Fax: () _____ - _____

Project Description: _____

Date: (Mo. & Yr.): From _____ To _____ Dollar Value of Project: \$_____

Client Name: _____ Client's Project Manager: _____

Address: _____ City: _____

State: _____ Zip: _____ Phone: () _____ - _____ Fax: () _____ - _____

Project Description: _____

Date: (Mo. & Yr.): From _____ To _____ Dollar Value of Project: \$_____

Client Name: _____ Client's Project Manager: _____

Address: _____ City: _____

State: _____ Zip: _____ Phone: () ____ - _____ Fax: () ____ - _____

Project Description: _____

Date: (Mo. & Yr.): From _____ To _____ Dollar Value of Project: \$_____

Client Name: _____ Client's Project Manager: _____

Address: _____ City: _____

State: _____ Zip: _____ Phone: () ____ - _____ Fax: () ____ - _____

Project Description: _____

Date: (Mo. & Yr.): From _____ To _____ Dollar Value of Project: \$_____

Client Name: _____ Client's Project Manager: _____

Address: _____ City: _____

State: _____ Zip: _____ Phone: () ____ - _____ Fax: () ____ - _____

Project Description: _____

Date: (Mo. & Yr.): From _____ To _____ Dollar Value of Project: \$_____

Client Name: _____ Client's Project Manager: _____

Address: _____ City: _____

State: _____ Zip: _____ Phone: () ____ - _____ Fax: () ____ - _____

Project Description: _____

Name of Business: _____

FORM MUST BE EXECUTED AND SUBMITTED WITH BID PACKAGE

**DRUG-FREE WORKPLACE PROGRAM,
VEHICLE OPERATOR LICENSE & VEHICLE REGISTRATION,
NOTICE OF INTENT TO SUBLET**

I, _____, _____
(Name) Owner, President or Designated Officer (Corp. Resolution*) (Title)
of _____, hereby certify that;
(Name of Business)

A. Drug-Free Workplace Program Certification

This firm ____ (has) ____ (has not) implemented a Drug-Free Workplace Program in accordance with the provision of Section 287.087, F.S.

B. Vehicle Operator License & Vehicle Registration

All operators driving Proposer vehicles are properly licensed in the State of Florida, for the type of vehicle being operated, in accordance with Chapter 322 F.S., and further states that all vehicles operated, or caused to be operated by said Proposer;

- Meet the financial responsibility requirements in accordance with Chapter 324 F.S., and shall remain so for the duration of the Contract.
- Registered in the State of Florida, in accordance with Section 337.11 F.S, and insured in the State of Florida to the limits required within the Contract and in accordance with Sections 320.02, 316.646, and 627.733 F.S., and shall remain so for the duration of the Contract.

C. Notice of Intent to Sublet

We ____ (do) ____ (do not) intend to sublet a portion of the work on this project.

If I have indicated above that a portion of the work will be sublet, then I hereby further certify that we have taken affirmative action to seek out and consider Minority Business Enterprises as potential subcontractors and/or suppliers. The classes of work I intend to sublet and the firms considered as potential subcontractors are as follows:

<u>Class of Work</u>	<u>Potential Subcontractors</u>	<u>Percent</u>	<u>MBE (Y) or (N)</u>
_____	_____	_____%	_____
_____	_____	_____%	_____
_____	_____	_____%	_____
_____	_____	_____%	_____

*Percentage must not be for more than 51% of contract total

Signature: _____ Date: _____
Owner, President or Designated Officer (Corp. Resolution*)

*If person signing the form is someone other than the Owner or President, a copy of the Corporate Resolution granting signature authorization must be furnished in the bid package.

FORM MUST BE EXECUTED AND SUBMITTED WITH THE PROPOSAL PACKAGE

CONTRACTOR NOTIFICATION

TO: All Contractors

FROM: Turnpike Asbestos Coordinator
(954) 975-4855
Pompano Beach, Florida

SUBJECT: ASBESTOS-CONTAINING MATERIALS IN TURNPIKE FACILITIES

It is possible that you may encounter Asbestos-containing materials (ACM) while working in State-owned buildings since ACM are present in many of these buildings. The presence of ACM does not necessarily mean that a hazard exists. However, a hazard may be created when ACM is disturbed and asbestos fibers become airborne. The best way to maintain a safe environment is to avoid disturbance of ACM.

Prominently posted in each building is an "Occupant Notification" which summarizes known locations of ACM in that building. An Operations and Maintenance (O & M) plan has been developed for these known locations of ACM. Since the known locations may or may not include all ACM, workers must exercise caution and be watchful for materials that might contain asbestos. You must avoid inadvertently disturbing ACM or suspected ACM as you carry out your work.

If you need additional information regarding ACM in a particular building or would like to see a copy of the O & M Plan, contact the Building Asbestos Contact Person (BACPer) responsible for that building or the Turnpike Asbestos Coordinator. The specific designated BACPer (name and telephone) is listed on the "Occupant Notification".

If your work necessitates the disturbance of ACM, you shall take all precautions necessary to protect human health and the environment from asbestos fibers. At a minimum, you must use the procedures found in the O & M Plan; comply with all federal, state and local laws governing work with asbestos; assure that your employees are medically certified, trained and equipped with the proper personal protective devices for safe handling of ACM; and ensure that all employees performing work with ACM related to State-owned buildings execute a "Certificate of Worker's Acknowledgment" prior to beginning work. Immediately upon inadvertently or before disturbing ACM in any State-owned building you must notify the designated BACPer.

ACKNOWLEDGMENT OF ASBESTOS WARNING

I, _____
(Name) Owner, President, or Designated Officer (Corp. Resolution*) (Title)

of _____, hereby acknowledge receipt of the above memorandum about
(Name of Business)

Asbestos-Containing Materials (ACM) Information for Turnpike Facilities and information on how to contact the Building Asbestos Contact Person (BACPer), for information regarding how to find out where asbestos-containing materials are located and how to avoid any contact with ACM.

Signature: _____
Owner, President, or Designated Officer (Corp. Resolution*)

Date: _____

* If person signing for the Business is someone other than the Owner, or President, a copy of the Corporate Resolution granting signature authorization must be furnished in the bid package.

FORM MUST BE EXECUTED AND SUBMITTED WITH THE PROPOSAL PACKAGE

CORPORATE RESOLUTION OF

(recite name of Business)

WHEREAS, it is in the best interests of this corporation to enter into a contract with the State of Florida, _____ Department _____ of _____ Transportation _____ for

NOW THEREFORE, IT IS RESOLVED, that _____ (title of authorized officer; (e.g., Vice President) of this Business is hereby authorized and empowered on behalf of the Business to enter into a contract with the State of Florida, Department of Transportation, in consideration of _____ Dollars (\$ _____), upon the terms and conditions contained in the proposed contract, a copy of which is attached hereto as Exhibit A, and made a part hereof.

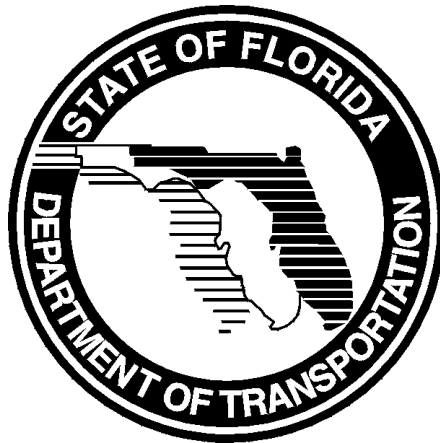
CERTIFICATE OF RESOLUTION

I, _____, secretary of _____ (name of Business), a Florida Business, or a Business founded in the State of _____, and authorized by the Secretary of State, State of Florida, to conduct business in the State of Florida, hereby certify that the foregoing is a full, true, and correct copy of the resolution of the Board of Directors of the Business, duly and regularly passed and adopted at a meeting of the Board duly called and held in all respects as required by law, and by the bylaws of the Business, on the _____ day of _____, 20____, at which meeting a quorum of the Board was present.

Executed by me as secretary of the corporation on this _____ day of _____, 20____.

Signature of Secretary

Name of Secretary printed or typed



STANDARD WRITTEN AGREEMENT

RFP-DOT- 09/10-8001-KB

PAYMENT CARD INDUSTRY (PCI) SERVICES

FPI No. 423249-1-32-01

STATE OF FLORIDA DEPARTMENT OF TRANSPORTATION
STANDARD WRITTEN AGREEMENT

Agreement No. _____
Financial Project ID 423429-1-32-01
Vendor No. _____
Procurement No. RFP-DOT-09/10-8001-KB
D.M.S. Catalog Class No. _____

BY THIS AGREEMENT, made and entered into this _____ day of _____, 2009, by and between the STATE OF FLORIDA DEPARTMENT OF TRANSPORTATION, hereinafter called "Department" and _____, duly authorized to conduct business in the State of Florida, hereinafter called "Vendor," hereby agree as follows:

1. SERVICES AND PERFORMANCE

- A. In connection with seeking a Vendor that is recognized and approved by the Payment Card Industry (PCI) Security Standards Council to provide PCI required services for a Level 1 merchant. These services will be required on an annual basis and are described in this Exhibit "A", attached hereto and made a part hereof.
- B. Before making any additions or deletions to the work described in this Agreement, and before undertaking any changes or revisions to such work, the parties shall negotiate any necessary cost changes and shall enter into an Amendment covering such work and compensation. Reference herein to this Agreement shall include any Amendment(s).
- C. All tracings, plans, specifications, maps, computer files and reports prepared or obtained under this Agreement, as well as all data collected, together with summaries and charts derived therefrom, shall be the exclusive property of the Department without restriction or limitation on their use and shall be made available, upon request, to the Department at any time during the performance of such services and/or upon completion or termination of this Agreement. Upon delivery to the Department of said document(s), the Department shall become the custodian thereof in accordance with Chapter 119, Florida Statutes. The Vendor shall not copyright any material and products or patent any invention developed under this Agreement. The Department shall have the right to visit the site for inspection of the work and the products of the Vendor at any time.
- D. All final plans, documents, reports, studies and other data prepared by the Vendor shall bear the professional's seal/signature, in accordance with the applicable Florida Statutes, Administrative Rules promulgated by the Department of Business and Professional Regulation, and guidelines published by the Department, in effect at the time of execution of this Agreement. In the event that changes in the Statutes or Rules create a conflict with the requirements of the published guidelines, requirements of the Statute and Rules shall take precedence.
- E. The Vendor agrees to provide project schedule progress reports in a format acceptable to the Department and at intervals established by the Department. The Department shall be entitled at all times to be advised, at its request, as to the status of work being done by the Vendor and of the details thereof. Coordination shall be maintained by the Vendor with representatives of the Department, or of other agencies interested in the project on behalf of the Department. Either party to the Agreement may request and be granted a conference.
- F. All services shall be performed by the Vendor to the satisfaction of the Director who shall decide all questions, difficulties and disputes of any nature whatsoever that may arise under or by reason of this Agreement, the prosecution and fulfillment of the services hereunder and the character, quality, amount of value thereof; and the decision upon all claims, questions and disputes shall be final and binding upon all parties hereto. Adjustments of compensation and contract time because of any major changes in the work that may become necessary or desirable as the work progresses shall be subject to mutual agreement of the parties, and Amendment(s) shall be entered into by the parties in accordance herewith.

Reference herein to the Director shall mean the Department's Deputy Executive Director, Florida's Turnpike Enterprise.

2. TERM

- A. Initial Term. This Agreement shall begin on date of execution and shall remain in full force and effect through completion of all services required or three (3) years from the date of the NTP, whichever occurs first. Subsequent to the execution of this Agreement by both parties, the services to be rendered by the Vendor shall commence and be completed in accordance with the option selected below. (Select box and indicate date(s) as appropriate):

☐ Services shall commence _____ and shall be completed by _____ or date of termination whichever occurs first.

☒ Services shall commence upon written notice from the Department's Contract Manager and shall be completed within three (3) years or date of termination, whichever occurs first.

☐ Other: See Exhibit "A"

- B. RENEWALS (Check appropriate box):

☐ This Agreement may not be renewed.

☒ This Agreement may be renewed for a period that may not exceed three (3) years or the term of the original contract, whichever period is longer. Renewals shall be contingent upon satisfactory performance evaluations by the Department and subject to the availability of funds. Any renewal or extension shall be in writing and executed by both parties, and shall be subject to the same terms and conditions set forth in this Agreement.

- C. EXTENSIONS. In the event that circumstances arise which make performance by the Vendor impracticable or impossible within the time allowed or which prevent a new contract from being executed, the Department, at its discretion, may grant an extension of this Agreement. Extension of this Agreement shall be in writing for a period not to exceed six (6) months and shall be subject to the same terms and conditions set forth in this Agreement; provided the Department may, at its discretion, grant a proportional increase in the total dollar amount based on the method and rate established herein. There shall be only one extension of this Agreement unless the failure to meet the criteria set forth in this Agreement for completion of this Agreement is due to events beyond the control of the Vendor.

It shall be the responsibility of the Vendor to ensure at all times that sufficient time remains in the Project Schedule within which to complete services on the project. In the event there have been delays that would affect the project completion date, the Vendor shall submit a written request to the Department which identifies the reason(s) for the delay and the amount of time related to each reason. The Department shall review the request and make a determination as to granting all or part of the requested extension.

3. COMPENSATION AND PAYMENT

- A. Payment shall be made only after receipt and approval of goods and services unless advance payments are authorized by the Chief Financial Officer of the State of Florida under Section 215.422(14), Florida Statutes.
- B. If this Agreement involves units of deliverables, then such units must be received and accepted in writing by the Contract Manager prior to payments.
- C. Bills for fees or other compensation for services or expenses shall be submitted in detail sufficient for a proper preaudit and postaudit thereof.
- D. Bills for any travel expenses, when authorized by terms of this Agreement and by the Department's Project Manager, shall be submitted in accordance with Section 112.061, Florida Statutes, and Chapter 3 - Travel, Department's Disbursement Operations Manual, 350-030-400.
- E. Vendors providing goods and services to the Department should be aware of the following time frames. Upon receipt, the Department has five (5) working days to inspect and approve the goods and services, unless otherwise specified herein. The Department has twenty (20) days to deliver a request for payment (voucher) to the Department of Financial Services. The twenty (20) days are measured from the latter of the date the invoice is received or the goods or services are received, inspected and approved.

- F. If a payment is not available within forty (40) days, a separate interest penalty as established pursuant to Section 215.422, Florida Statutes, shall be due and payable, in addition to the invoice amount, to the Vendor. Interest penalties of less than one (1) dollar shall not be enforced unless the Vendor requests payment. Invoices which have to be returned to a Vendor because of Vendor preparation errors shall result in delay of payment. The invoice payment requirements do not start until a properly completed invoice is provided to the Department.
- G. The State of Florida, through the Department of Management Services, has instituted MyFloridaMarketPlace, a Statewide eProcurement system. Pursuant to Section 287.057(23), Florida Statutes, all payments shall be assessed a transaction fee of one percent (1%), which the Vendor shall pay to the State. For payments within the State accounting system (FLAIR or its successor), the transaction fee shall, when possible, be automatically deducted from payments to the Vendor. If automatic deduction is not possible, the Vendor shall pay the transaction fee pursuant to Rule 60A-1.031(2), Florida Administrative Code. By submission of these reports and corresponding payments, Vendor certifies their correctness. All such reports and payments shall be subject to audit by the State or its designee. The Vendor shall receive a credit for any transaction fee paid by the Vendor for the purchase of any item(s) if such item(s) are returned to the Vendor through no fault, act, or omission of the Vendor. Notwithstanding the foregoing, a transaction fee is non-refundable when an item is rejected or returned, or declined, due to the Vendor's failure to perform or comply with specifications or requirements of the Agreement. Failure to comply with these requirements shall constitute grounds for declaring the Vendor in default and recovering procurement costs from the Vendor in addition to all outstanding fees. VENDORS DELINQUENT IN PAYING TRANSACTION FEES MAY BE EXCLUDED FROM CONDUCTING FUTURE BUSINESS WITH THE STATE.
- H. A Vendor Ombudsman has been established within the Department of Financial Services. The duties of this individual include acting as an advocate for vendors who may be experiencing problems in obtaining timely payment(s) from a state agency. The Vendor Ombudsman may be contacted at (850) 413-5516 or by calling the State Comptroller's Hotline, 1-877-693-5236.
- I. Records of costs incurred under terms of this Agreement shall be maintained and made available upon request to the Department at all times during the period of this Agreement and for three (3) years after final payment for the work pursuant to this Agreement is made. Copies of these documents and records shall be furnished to the Department upon request. Records of costs incurred shall include the Vendor's general accounting records and the project records, together with supporting documents and records, of the Vendor and all subcontractors performing work on the project, and all other records of the Vendor and subcontractors considered necessary by the Department for a proper audit of project costs.
- J. The Department, during any fiscal year, shall not expend money, incur any liability, or enter into any contract which, by its terms, involves the expenditure of money in excess of the amounts budgeted as available for expenditure during such fiscal year. Any contract, verbal or written, made in violation of this subsection is null and void, and no money may be paid on such contract. The Department shall require a statement from the Comptroller of the Department that funds are available prior to entering into any such contract or other binding commitment of funds. Nothing herein contained shall prevent the making of contracts for periods exceeding one (1) year, but any contract so made shall be executory only for the value of the services to be rendered or agreed to be paid for in succeeding fiscal years. Accordingly, the Department's performance and obligation to pay under this Agreement is contingent upon an annual appropriation by the Legislature.

4. INDEMNITY AND PAYMENT FOR CLAIMS

- A. INDEMNITY: The Vendor shall indemnify and hold harmless the Department, its officers and employees, from liabilities, damages, losses and costs, including, but not limited to, reasonable attorney's fees, to the extent caused by negligence, recklessness, or intentional wrongful misconduct of the Vendor and persons employed or utilized by the Vendor in the performance of this Agreement.

It is specifically agreed between the parties executing this Agreement that it is not intended by any of the provisions of any part of the Agreement to create in the public or any member thereof, a third party beneficiary hereunder, or to authorize anyone not a party to this Agreement to maintain a suit for personal injuries or property damage pursuant to the terms or provisions of this Agreement.

PAYMENT FOR CLAIMS: The Vendor guarantees the payment of all just claims for materials, supplies, tools, or labor and other just claims against the Vendor or any subcontractor, in connection with the Agreement. The Department's final acceptance and payment does not release the Vendor's bond until all such claims are paid or released.

- B. LIABILITY INSURANCE. (Check and complete as appropriate):

- ☒ [X] No general liability insurance required.
- ☐ [] The Vendor shall carry and keep in force during the term of this Agreement a general liability insurance policy or policies with a company or companies authorized to do business in Florida, affording public liability insurance with combined bodily injury limits of at least \$ _____ per person and \$ _____ each occurrence, and property damage insurance of at least \$ _____ each occurrence, for the services to be rendered in accordance with this Agreement.
- ☐ [] The Vendor shall have and maintain during the period of this Agreement, a professional liability insurance policy or policies or an irrevocable letter of credit established pursuant to Chapter 675 and Section 337.106, Florida Statutes, with a company or companies authorized to do business in the State of Florida, affording liability coverage for the professional services to be rendered in accordance with this Agreement in the amount of \$ _____.
- ☐ [] The Vendor shall carry and keep in force during the period of this Agreement a Pollution Liability Insurance Policy in the amount of not less than one million dollars (\$1,000,000.00).
- C. WORKER'S COMPENSATION. The Vendor shall also carry and keep in force Workers' Compensation insurance as required for the State of Florida under the Workers' Compensation Law.
- D. PERFORMANCE AND PAYMENT BOND. (Check as appropriate):
- ☒ [X] No Bond required.
- ☐ [] Prior to commencement of any services pursuant to this Agreement and at all times during the term hereof, including renewals and extensions, the Vendor shall supply to the Department and keep in force a bond provided by a surety authorized to do business in the State of Florida, payable to the Department and conditioned for the prompt, faithful, and efficient performance of this Agreement according to the terms and conditions hereof and within the time periods specified herein, and for the prompt payment of all persons furnishing labor, materials, equipment and supplies therefore.
- E. CERTIFICATION. With respect to any insurance policy required pursuant to this Agreement, all such policies shall be issued by companies licensed to do business in the State of Florida. The Vendor shall provide to the Department certificates showing the required coverage to be in effect and showing the Department to be an additional certificate holder. Such policies shall provide that the insurance is not cancelable except upon thirty (30) days prior written notice to the Department.

5. COMPLIANCE WITH LAWS

- A. The Vendor shall allow public access to all documents, papers, letters, or other material subject to the provisions of Chapter 119, Florida Statutes, and made or received by the Vendor in conjunction with this Agreement. Failure by the Vendor to grant such public access shall be grounds for immediate unilateral cancellation of this Agreement by the Department.
- B. The Vendor agrees that it shall make no statements, press releases or publicity releases concerning this Agreement or its subject matter or otherwise disclose or permit to be disclosed any of the data or other information obtained or furnished in compliance with this Agreement, or any particulars thereof, during the period of the Agreement, without first notifying the Department's Contract Manager and securing prior written consent. The Vendor also agrees that it shall not publish, copyright or patent any of the data developed under this Agreement, it being understood that such data or information are works made for hire and the property of the Department.
- C. The Vendor shall comply with all federal, state and local laws and ordinances applicable to the work or payment for work thereof, and shall not discriminate on the grounds of race, color, religion, sex, national origin, age, or disability in the performance of work under this Agreement.
- D. If the Vendor is licensed by the Department of Business and Professional Regulation to perform the services herein contracted, then Section 337.162, Florida Statutes, applies as follows:
- (1) If the Department has knowledge or reason to believe that any person has violated the provisions of state professional licensing laws or rules, it shall submit a complaint regarding the violations to the Department of Business and Professional Regulation. The complaint shall be confidential.

- (2) Any person who is employed by the Department and who is licensed by the Department of Business and Professional Regulation and who, through the course of the person's employment, has knowledge to believe that any person has violated the provisions of state professional licensing laws or rules shall submit a complaint regarding the violations to the Department of Business and Professional Regulation. Failure to submit a complaint about the violations may be grounds for disciplinary action pursuant to Chapter 455, Florida Statutes, and the state licensing law applicable to that licensee. The complaint shall be confidential.
- (3) Any complaints submitted to the Department of Business and Professional Regulation are confidential and exempt from Section 119.07(1), Florida Statutes, pursuant to Chapter 455, Florida Statutes, and applicable state law.
- E. The Vendor covenants and agrees that it and its employees shall be bound by the standards of conduct provided in applicable Florida Statutes and applicable rules of the Board of Business and Professional Regulation as they relate to work performed under this Agreement. The Vendor further covenants and agrees that when a former state employee is employed by the Vendor, the Vendor will require that strict adherence by the former state employee to Florida Statutes 112.313 and 112.3185 is a condition of employment for said former state employee. These statutes will by reference be made a part of this Agreement as though set forth in full. The Vendor agrees to incorporate the provisions of this paragraph in any subcontract into which it might enter with reference to the work performed pursuant to this Agreement.
- F. A person or affiliate who has been placed on the convicted vendor list following a conviction for a public entity crime may not submit a bid, proposal or reply on a contract to provide any goods or services to a public entity, may not submit a bid, proposal or reply on a contract with a public entity for the construction or repair of a public building or public work, may not submit bids, proposals or replies on leases of real property to a public entity, may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity, and may not transact business with any public entity in excess of the threshold amount provided in Section 287.017, Florida Statutes, for CATEGORY TWO for a period of thirty-six (36) months following the date of being placed on the convicted vendor list.
- G. An entity or affiliate who has been placed on the discriminatory vendor list may not submit a bid, proposal or reply on a contract to provide any goods or services to a public entity, may not submit a bid, proposal or reply on a contract with a public entity for the construction or repair of a public building or public work, may not submit bids, proposals or replies on leases of real property to a public entity, may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity, and may not transact business with any public entity.
- H. The Department shall consider the employment by any Vendor of unauthorized aliens a violation of Section 274A(e) of the Immigration and Nationality Act. If the Vendor knowingly employs unauthorized aliens, such violation shall be cause for unilateral cancellation of this Agreement.
- I. Pursuant to Section 216.347, Florida Statutes, the Vendor may not expend any State funds for the purpose of lobbying the Legislature, the Judicial Branch, or State Agency.

6. TERMINATION AND DEFAULT

- A. This Agreement may be canceled by the Department in whole or in part at any time the interest of the Department requires such termination. The Department further reserves the right to terminate or cancel this Agreement in the event an assignment be made for the benefit of creditors.
- B. If the Department determines that the performance of the Vendor is not satisfactory, the Department shall have the option of (a) immediately terminating the Agreement, or (b) notifying the Vendor of the deficiency with a requirement that the deficiency be corrected within a specified time, otherwise the Agreement will be terminated at the end of such time, or (c) take whatever action is deemed appropriate by the Department.
- C. If the Department requires termination of the Agreement for reasons other than unsatisfactory performance of the Vendor, the Department shall notify the Vendor of such termination, with instructions as to the effective date of termination or specify the stage of work at which the Agreement is to be terminated.
- D. If the Agreement is terminated before performance is completed, the Vendor shall be paid only for that work satisfactorily performed for which costs can be substantiated. Such payment, however, may not exceed an amount that is the same percentage of the agreement price as the amount of work satisfactorily completed is a percentage of the total work called for by this Agreement. All work in progress shall become the property of the Department and shall be turned over promptly by the Vendor.

7. ASSIGNMENT AND SUBCONTRACTS

A. The Vendor shall maintain an adequate and competent staff so as to enable the Vendor to timely perform under this Agreement and may associate with it such subcontractors, for the purpose of its services hereunder, without additional cost to the Department, other than those costs within the limits and terms of this Agreement. The Vendor is fully responsible for satisfactory completion of all subcontracted work. The Vendor, however, shall not sublet, assign or transfer any work under this Agreement to other than subcontractors specified in the proposal, bid and/or Agreement without consent of the Department.

B. Select the appropriate box:

☒ [X] The following provisions is not applicable to this Agreement.

☐ [] The following provision is hereby incorporated in and made a part of this Agreement:

It is expressly understood and agreed that any articles which are the subject of, or required to carry out this Agreement shall be purchased from a nonprofit agency for the blind or for the severely handicapped that is qualified pursuant to Chapter 413, Florida Statutes, in the same manner and under the same procedures set forth in Section 413.036(1) and (2), Florida Statutes; and for purposes of this Agreement, the person, firm, or other business entity (Vendor) carrying out the provisions of this Agreement shall be deemed to be substituted for the State Agency (Department) insofar as dealings with such qualified nonprofit agency are concerned.

☐ [] The following provision is hereby incorporated in and made a part of this Agreement:

It is expressly understood and agreed that any articles that are the subject of, or required to carry out this Agreement shall be purchased from the corporation identified under Chapter 946, Florida Statutes, in the same manner and under the procedures set forth in Section 946.515(2) and (4), Florida Statutes; and for purposes of this Agreement the person, firm, or other business entity (Vendor) carrying out the provisions of this Agreement shall be deemed to be substituted for this Agency (Department) insofar as dealings with such corporation is concerned.

The "corporation identified" is Prison Rehabilitative Industries and Diversified Enterprises, Inc. (PRIDE). Available pricing, products, and delivery schedules may be obtained by contacting:

PRIDE Enterprises
12425 - 28th Street North
St. Petersburg, Florida 33716-1826
Telephone: (800) 643-8459

☐ [] This Agreement involves the expenditure of Federal funds and Section 946.515, Florida Statutes, as noted above, does not apply. However, Appendix I is applicable to all parties and is hereof made a part of this Agreement.

8. MISCELLANEOUS

A. The Vendor and its employees, agents, representatives, or subcontractors are not employees of the Department and are not entitled to the benefits of State of Florida employees. Except to the extent expressly authorized herein, Vendor and its employees, agents, representatives, or subcontractors are not agents of the Department or the State for any purpose or authority such as to bind or represent the interests thereof, and shall not represent that it is an agent or that it is acting on the behalf of the Department or the State. The Department shall not be bound by any unauthorized acts or conduct of the Vendor or its employee, agents, representatives, or subcontractor. Vendor agrees to include this provision in all its subcontracts under this Agreement.

B. All words used herein in the singular form shall extend to and include the plural. All words used in the plural form shall extend to and include the singular. All words used in any gender shall extend to and include all genders.

C. This Agreement embodies the whole agreement of the parties. There are no promises, terms, conditions, or obligations other than those contained herein, and this Agreement shall supersede all previous communications, representations, or agreements, either verbal or written, between the parties hereto. The State of Florida terms and conditions, whether general or specific, shall take precedence over and supersede any inconsistent or conflicting provision in any attached terms and conditions of the Vendor.

- D. It is understood and agreed by the parties hereto that if any part, term or provision of this Agreement is by the courts held to be illegal or in conflict with any law of the State of Florida, the validity of the remaining portions or provisions shall not be affected, and the rights and obligations of the parties shall be construed and enforced as if the Agreement did not contain the particular part, term or provision held to be invalid.
- E. This Agreement shall be governed by and construed in accordance with the laws of the State of Florida.
- F. In any legal action related to this Agreement, instituted by either party, the Vendor hereby waives any and all privileges and rights it may have under Chapter 47 and Section 337.19, Florida Statutes, relating to venue, as it now exists or may hereafter be amended, and any and all such privileges and rights it may have under any other statute, rule, or case law, including, but not limited to those grounded on convenience. Any such legal action may be brought in the appropriate Court in the county chosen by the Department and in the event that any such legal action is filed by the Vendor, the Vendor hereby consents to the transfer of venue to the county chosen by the Department upon the Department filing a motion requesting the same.
- G. If this Agreement involves the purchase of maintenance of information technology, as defined in Section 282.0041, Florida Statutes, Appendix II may be applicable, and is made a part of this Agreement, if attached.
- H. Time is of the essence as to each and every obligation under this Agreement.
- I. The following attachments are incorporated and made a part of this Agreement. In case of discrepancy in any of the provisions of these attachments with this Standard Written Agreement, the provisions of this Standard Written Agreement shall govern. In case of discrepancy, the attachments are listed in governing order as follows:
Exhibit "A," Exhibit "B", Exhibit "C", Attachments , PUR 1000 and PUR 1001.

IN WITNESS WHEREOF, the parties have executed this Agreement by their duly authorized officers on the day, month and year set forth above.

STATE OF FLORIDA
DEPARTMENT OF TRANSPORTATION

(Name of Vendor)

By: _____
(Authorized Signature)

(Print/Type Name)

Title: _____
(President / Owner)

By: _____

James L. Ely

(Print/Type Name)

Title: Executive Director and Chief Executive Officer

FOR DEPARTMENT USE ONLY

APPROVED:

Procurement Office

LEGAL APPROVAL:

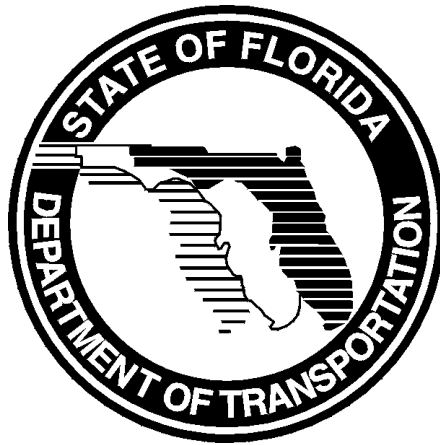


EXHIBIT "A"

SCOPE OF SERVICES

RFP-DOT- 09/10-8001-KB

PAYMENT CARD INDUSTRY (PCI) SERVICES

FPI No. 423249-1-32-01

EXHIBIT "A"
SCOPE OF SERVICES
PAYMENT CARD INDUSTRY (PCI) SERVICES

1. INTRODUCTION

1.1 Description of Services

The Florida Department of Transportation, Turnpike Enterprise, hereinafter referred to as the "Department," requires a Vendor that is recognized and approved by the PCI Security Standards Council to provide Payment Card Industry (PCI) required services for a Level 1 merchant. These services will be required on an annual basis and are described in this Exhibit. Any additional services above and beyond the minimum PCI Data Security Standards (DSS) to ensure an annual passing report of compliance are welcomed.

2. BACKGROUND

Florida's Turnpike is a four hundred sixty (460) mile toll road, consisting of a three hundred and twenty (320) mile mainline, extending from Wildwood in central Florida to Miami, and several expansion projects, totaling one hundred forty (140) miles, in operation in Central Florida, the Tampa Bay region and Broward county.

House Bill (HB) 261, signed by former Governor Bush on April 11, 2001, created Florida's Turnpike Enterprise, merging the Department's Office of Toll Operations, which collects the toll revenues, with the Turnpike System into a single administrative unit.

In 2008, the Department obtained its PCI Level 1 merchant report of compliance, had over seventy thousand (70,000) credit card transactions per day (approx. twenty-five million (25,000,000) transactions per year), revenues exceeded six hundred eighty four million (\$684,000,000) and sold over four million (4,000,000) transponders through the SunPass pre-paid tolling program.

The Department operates a medium sized heterogeneous IT environment with approximately four thousand (4000) nodes in total. Its major operating platforms/systems are open VMS, Solaris, and Windows. There are two (2) call centers with access to the Department data bases (Boca and Orlando). The Boca call center has approximately one hundred (100) agents and the Orlando call center approximately one hundred –thirty (130). The IT staff which is located in both Boca and Orlando contains approximately one hundred (100) people. Approximately three hundred (300) people have concurrent access to the data bases.

The Department's credit card application is an electronic toll collection (SunPass) and its primary data center is located in Boca Raton, Florida. There is also a call center located in Boca Raton. Additionally there are two (2) other locations in Orlando, Florida approximately two hundred (200) miles away. One (1) center is the Orlando recovery site and the other is the Orlando call center. These two (2) facilities are approximately ten (10) miles apart. The primary web site through which users enter credit card numbers is currently housed internally.

The Department's wide area network is fiber and some frame relay based. A ten (10) GB backbone runs from Boca to the Orlando data center. There are HP OpenVMS Sun Solaris based servers and Windows based servers/pcs in the credit card environment. There is also an IVR connection to the database.

3. ASSUMPTIONS/CONSTRAINTS

- 3.1 Work will be commencing within the third calendar quarter of 2009. The Department will select the start date and provide approximately one (1) month lead time.
- 3.2 Vendor must be or employ a PCI Qualified Security Assessor (QSA), PCI Approved Scanning Vendor (ASV) and a qualified forensic expert that is a Visa-approved Qualified Incident Response Assessor (QIRA). All subcontractors must be approved by the Department.
- 3.3 Vendor must be qualified to do business in the State of Florida.
- 3.4 All work performed must be in accordance with PCI specified procedures for the PCI annual onsite security audit.
- 3.5 PCI specified procedures for meeting or exceeding the PCI DSS Requirement 11.2, 11.3, 11.3.1, 11.3.2 and 6.6 with tests that include the vulnerabilities listed in Requirement 6.5.
- 3.6 All deliverables must be in accordance with PCI specified requirements with all reports being acceptable by the onsite PCI auditor and acquiring bank.
- 3.7 All work performed and deliverables must be kept confidential per a non-disclosure agreement.
- 3.8 Vendor must have completed at least two (2) successful PCI audits for Level 1 merchants.
- 3.9 Vendor must provide at least two (2) references (Level 1 merchants) in which PCI engagements were performed.
- 3.10 Vendor must submit resumes of the service providers (i.e. QSA, ASV, and Forensic SME, etc.).
- 3.11 Vendor must submit a sample report of each type of deliverable proposed.

4. SCOPE OF SERVICES

To be eligible, the work must be performed by a QSA and an ASV that is recognized by the PCI Security Standards Council.

(https://www.pcisecuritystandards.org/qa_asv/find_one.shtml).

The objective is to meet all requirements set forth and outlined by the PCI DSS that requires an external or third-party engagement

(https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html)).

The following engagements are being procured at a fixed lump sum price:

- PCI audit services (by a QSA) to meet PCI annual requirements,
- Network Penetration Test (Network-Layer) to include wireless discovery and war dial to meet PCI DSS requirement 11.3 and 11.3.1,
- Web application penetration / application-layer specific penetration test that meets PCI DSS requirements 6.6, 11.3 and 11.3.2,
- Quarterly network scanning services (by a QSV) to meet PCI DSS requirement 11.2,
- Business Impact Analysis.

Forensic Security Services and PCI audit services (remediation consulting) will require a fixed hourly rate if additional hours outside of defined scope are required.

A detailed report as described below will be required at the conclusion of each engagement. The engagements are normally scheduled during the third quarter of each calendar year unless stated differently in the detailed description.

At a minimum, the following engagements must meet the listed Scopes:

4.1 **PCI Audit Services:**

4.1.1 Objective

The Department is seeking a PCI QSA Vendor to perform an annual on site PCI security audit as per PCI requirements.

The Vendor shall follow a standard audit process of reviewing security policies, interviewing key staff to understand existing controls and performing verification through documentation or console review. The Vendor will then produce an Initial Report of Compliance (IROC) identifying areas of non-compliance to the PCI standard and provide high-level remediation recommendations or compensating controls to meet the standard. Once the Department has completed all remediation efforts, the Vendor will issue a Report of Compliance (ROC). The Vendor will also respond to questions and provide PCI DSS requirements clarification, when required, for the duration of the contract. Occasionally the Department may seek a QSA's professional opinion or their interpretation of a PCI requirement.

4.1.2 Scope

The Vendor shall perform an on-site PCI security audit and assess the Department's compliance with the requirements established by the PCI Security Standards Council. For areas that are found not in compliance with the requirements, the Vendor shall make recommendations to bring the Department in compliance and strengthen its overall security program for those areas.

4.1.3 Work Approach

Vendor must specify its project management and technical approach for this engagement. It is recommended that this engagement be comprised of the following four (4) phases of work:

Phase I - Pre-Assessment Activities

Phase II - On-Site Interviews

Phase III - Control Verification Review

Phase IV - PCI DSS v1.2 Assessment Documentation

4.1.4 Deliverables

Deliverables and documentation to be produced by Vendor are as follows:

Initial Report on Compliance (IROC): The IROC will provide details on any non-compliance issues against applicable PCI DSS v1.2 standards the Vendor discovered in the Department's security posture. Vendor will then schedule a meeting with the Department to explain, review and discuss the IROC and make corrections, if necessary.

Vendor shall issue an IROC to the Department after the onsite validation is completed. The IROC will provide the Department with details of the Vendor's findings and allow them to comment and make corrections if necessary. At this time, the Vendor will again instruct the Department to submit the Visa-developed "Status Compliance Form" to Visa, indicating that the appropriate level of corrective measures are underway. From this point forward, the Department is aware that they will be required to file quarterly status updates with Visa until compliance is fully achieved.

Should the Department not comply with certain PCI standards but utilize an alternate solution to accomplish what is intended by those PCI standards, the Vendor will work with the Department to clarify and develop these compensating controls. Provided the Vendor proves that such alternate solution appears to accomplish what is intended by the PCI standards, the Vendor will forward to the Department's acquiring bank or the PCI Council an explanation of the solution and why the Vendor deems it to include sufficient compensating controls to satisfy the relevant PCI standards.

The final determination of compliance on these alternatives, or exception items, resides with the acquiring bank or the PCI Council. In the event that the Department does not comply with certain PCI standards and no compensating controls are in place, the Department is required to take corrective measures. The IROC will provide high-level recommendations in this respect.

Report on Compliance (ROC): Subject to compliance, the Vendor will issue a ROC to the Department, or depending on the Department's PCI procedures, to the PCI Council.

Once all of the items deemed non-compliant in the IROC are brought into compliance, a final report on compliance is issued by the Vendor. Per Visa's requirements, this report is sent to Visa, the customer and their acquirer stating that the customer is fully compliant. Likewise, a statement of compliance is issued to MasterCard, AMEX and Discover Card (if required).

In the event the Department is not compliant, the Department may send information regarding their efforts to become compliant to the Vendor consultants for a period of one hundred and twenty (120) calendar days from the date of the IROC. If the Department has become compliant within this period, the Vendor will issue the ROC to the Department.

If the PCI DSS v1.2 standard requirements are not met within the aforementioned period of one hundred and twenty (120) days, the Department will require a follow-up assessment. The Department will have an opportunity for such a follow-up assessment, at an additional cost if required, which must be performed within two hundred and forty (240) calendar days from the date of the IROC. If PCI DSS v1.2 standard requirements are not met within this period of two hundred and forty (240) days, a new PCI assessment will need to be conducted for the purposes of the Vendor being able to attest compliance. These timeframes noted are necessary in order to review any changes or updates in the environment that may have occurred since the original on-site assessment was conducted. As such, a new PCI assessment will be required and subject to a separate, additional order.

Completion of the above tasks is based on the following assumptions and the timely completion of the following the Department obligations:

The Department will provide Vendor existing security policies, standards, and procedures.

The Department will provide Vendor necessary documentation of the existing in-scope network configuration, servers, application, and security devices.

The Department will make the in-scope finance, IT, application, database, legal, audit, HR and physical security teams available for interviews with Vendor consultants.

The Department will provide information that is accurate and timely.

Any Department delays may impact the timeframe of the project.

4.2 Network Penetration Test (Network-Layer):

4.2.1 Objective

The Department is seeking a PCI ASV to perform an annual Network Penetration Test as per PCI requirements 11.3 and 11.3.1 for a Level 1 merchant.

The network penetration test identifies network and host based security vulnerabilities on the Department network infrastructures. Special emphasis is placed on systems identified by the Department as containing important information, which could include systems which provide a customer presence, process orders, or facilitate communication.

4.2.2 Scope

The Vendor shall perform a network penetration test. The Vendor will also assess the Department's compliance with the requirements established by the PCI Security Standards Council. For areas that are found not in compliance with the requirements, the Vendor will make recommendations to bring the Department into compliance and strengthen its overall security program.

Network Penetration Test which includes:

External Network Penetration Test (Per PCI DSS requirements 11.3 and 11.3.),
Wireless Discovery Assessment and War Dial Assessment.

4.2.3 Work Approach

Vendor must specify its project management and technical approach for this engagement.

4.2.4 Deliverables

Deliverables and documentation to be produced by Vendor are as follows:

After active testing has concluded, the Vendor will provide a detailed report that outlines discovered vulnerabilities in order of risk. Each finding includes a description of the vulnerability and its impact on security risk, as well as recommended remediation steps. Screen shots, log excerpts, and other technical evidence may be included, when applicable.

Documentation to be produced by the Department and Department obligations:

The Department will make available all necessary personnel to Vendor during the period of performance.

The Department understands that the following must be provided to Vendor, seventy two (72) hours or more prior to the scheduled commencement of this engagement:

Addresses of, and appropriate access to networked devices to be tested within the scope of the assessment, a list of appropriate contact personnel with “after hours” emergency contacts numbers, a list of phone numbers for the modem testing and appropriate on-site authorization documentation.

4.3 Web Application Penetration/ Application- Layer Specific Penetration Test

4.3.1 Objective

The Department is seeking a PCI QSA Vendor to perform a web application penetration test / application layer specific penetration test as per PCI requirements 11.3, 11.3.2 and 6.6 with tests that include the vulnerabilities listed in Req. 6.5. The Department is a Level 1 merchant. Its credit card application is a component of the electronic toll collection system (Sunpass) and its primary data center is located in Boca Raton, Florida. There is also a call center located in Boca Raton. Additionally there are two (2) other locations in Orlando, Florida approximately two hundred (200) miles away. One (1) center is the Orlando recovery site and the other is the Orlando call center. These two (2) facilities are approximately ten (10) miles apart. The primary web site through which users enter credit card numbers is currently housed internally.

4.3.2 Scope

The Vendor shall perform a Web Application Penetration Test / Application Layer Specific Penetration Test. The Vendor will also assess the Department’s compliance with the requirements established by the PCI Security Standards Council with emphasis on requirements 11.3, 11.3.2 and 6.6 with tests that include the vulnerabilities listed in Req. 6.5. For areas that are found out of compliance with the requirements, the Vendor will make recommendations to bring the Department in compliance and strengthen its overall security program.

A Web Application Penetration Test / Application Layer Specific Penetration Test identifies possible vulnerabilities in applications residing on networked servers and client workstations that offer user or inter-process interfaces, such as web applications and “thick” clients. The QSA’s assessment examines a customer application’s components and technologies to identify security vulnerabilities in client systems (such as web browsers), server systems (such as web servers, authentication technologies, application and database servers), static content (such as HTML pages and images), and server-side programs that implement the application logic (such as CGI (common gateway interface) scripts, ASP/PHP/Perl code and Java Servlets).

The QSA’s methodology should seek to identify two (2) general sets of application security vulnerabilities. The QSA shall test for common security vulnerabilities, such as stack overflows and format string issues, which may be discovered and exploited without intimate knowledge of the application’s design. In addition, the QSA examines the application’s underlying design for

unique security vulnerabilities that may not be easily recognizable during a more superficial investigation.

A variety of checks are performed, based on industry-specific guidance, best practices and standards. For example, application components may be tested for improper configuration, session tracking weaknesses, encryption implementation and strength, input validation, flaws in server-side executables, and sensitive or unnecessary information within Hyper Text Markup Language (HTML) content.

For the department, the QSA will perform an application vulnerability assessment of the application named www.sunpass.com.

This engagement will be conducted during the Department's normal business hours, as well as during designated off-hour windows.

Some testing can take place from a QSA testing location and on-site.

The following at a minimum should be conducted:

The Application Penetration Test consists of four significant phases, as follows:

Active host identification (Uniformed Device Discovery) - Establish a profile of all IP subnets in scope of the penetration test and identify the active devices within those subnets.

Vulnerability Scanning - Analyze available network services, and the IP stack fingerprints of active devices identified in the first phase.

Vulnerability Validation - Attempt to validate the results of the vulnerability scanning phase in order to both identify (and disregard) false-positive results, and validate other positive results from automated testing.

Exploitation - Once an understanding of device roles, potential trust relationships, accessible network services, potential vulnerabilities and Department approved targets is established, Vendor will attempt to gain access to target systems.

The Vendor and Department will jointly select a host or device of a particular operating system/vulnerability group for attempted exploitation. The Vendor will coordinate this work with appropriate Department staff in order to reduce the likelihood of undesired operational impacts to the Department.

Application Layer Specific Penetration Tests:

The Vendor shall perform security testing of the application by attempting to exploit identified vulnerabilities. Examples of testing techniques that may be used are as follows:

Input validation bypass – Client side validation routines and bounds-checking restrictions are removed to ensure controls are implemented on all application parameters sent to the server.

SQL injection – Specially crafted SQL commands are submitted in input fields to validate that input controls are in place to properly protect database data.

Cross-site scripting – Active content is submitted to the application in an attempt to cause a user's web browser to execute unauthorized and unfiltered code. This test is meant to validate user input controls.

Parameter tampering - Query strings, POST parameters, and hidden fields are modified in an attempt to gain unauthorized access to user data or application functionality.

Cookie poisoning – Data sent in cookies is modified in order to test application response to receiving unexpected cookie values.

Session hijacking – Attempt to take over a session established by another user and assume the privileges of that user.

User privilege escalation – Attempt to gain unauthorized access to administrator or other users' privileges.

Credential manipulation – Modify identification and authorization credentials in an attempt to gain unauthorized access to other users' data and application functionality.

Forceful browsing – Enumerate files located on a web server in an attempt to access files and user data not explicitly shown to the user within the application interface.

Backdoors and debug options – Many applications contain code left by developers for debugging purposes. Debugging code typically runs with a higher level of access, making it a target for potential exploitation. Application developers may leave backdoors in their code. The Vendor will identify these options that could potentially allow an intruder to gain additional levels of access.

Configuration subversion – Improperly configured web servers and application servers are common attack vectors. The Vendor assesses the software features, as well as the application and server configuration for poor configurations.

Perform a Web Application Penetration Test on Customer's URL:
www.sunpass.com

4.3.3 Work Approach

Vendor must specify its project management and technical approach for this engagement.

4.3.4 Deliverables

Deliverables and documentation to be produced by Vendor:

After active testing has concluded, the Vendor will provide a detailed report that outlines discovered vulnerabilities in order of risk. Each finding includes a description of the vulnerability and its impact on security risk, as well as recommended remediation steps. Screen shots and log excerpts may be included, when applicable.

Each Web Application Penetration Test / Application Layer Specific Penetration Test includes an Executive Summary, which contains a high-level analysis of the results of the assessment. Key findings are discussed, and graphs and charts break down findings by severity and difficulty, as well as by root cause. The overall results and security posture of the application are analyzed, with specific, high level recommendations for remediation of vulnerabilities and proactively preventing future application security issues.

Documentation to be produced by the Department and Department obligations:

The Department will make available all necessary personnel to Vendor during the period of performance.

The Department understands that the following must be provided to Vendor, seventy two (72) hours or more prior to the scheduled commencement of this engagement:

A list of appropriate contact personnel with "after hours" emergency contacts numbers and appropriate on-site authorization documentation.

4.4 **Quarterly Network Scanning Services:**

4.4.1 Objective

The Department is seeking a PCI QSA Vendor to perform Quarterly Network Penetration Tests as per PCI requirement 11.2. The Department is a Level 1 merchant and required to report to the acquiring bank on a quarterly basis. An

external network penetration test identifies network and host based security vulnerabilities on the Department network infrastructures. Special emphasis is placed on systems identified by the Department as containing important information, which could include systems which provide a customer presence, process orders, or facilitate communication.

4.4.2 Scope

The Vendor shall perform an external and internal vulnerability scan on a quarterly basis to ensure the requirements established by the PCI Security Standards Council (Requirement 11.2) are met. For areas that are not in compliance with the requirements, the Vendor will make recommendations to bring the Department into compliance and re-scan once remediated.

4.4.3 Work Approach

Vendor must specify its project management and technical approach for this engagement.

4.4.4 Deliverables

Deliverables and documentation to be produced by Vendor:

After active testing has concluded, the Vendor will provide a detailed report that outlines discovered vulnerabilities in order of risk. Each finding includes a description of the vulnerability and its impact on security risk, as well as recommended remediation steps. Screen shots and log excerpts may be included, when applicable. An executive report for external reporting is also required.

Documentation to be produced by the Department and the Department obligations:

The Department will make available all necessary personnel to Vendor during the period of performance.

The Department understands that the following must be provided to Vendor, seventy two (72) hours or more prior to the scheduled commencement of this engagement:

Addresses of, and appropriate access to networked devices to be tested within the scope of the assessment and a list of appropriate contact personnel with “after hours” emergency contacts numbers.

4.5 **Forensic Security Services:**

4.5.1 Objective

The Department is seeking a Visa-approved Qualified Incident Response Assessor (QIRA) Vendor on an annual retainer basis to perform forensic services as required, based on forty (40) hours per year with unused hours from

each year rolling over. The Department is a Level 1 merchant and required to report to the Acquiring Bank all breaches of its network and information systems. Having a Vendor that can provide Forensic Services after a security breach is suspected will help the Department to meet its reporting obligations to the Acquiring bank. Special emphasis is placed on systems identified by the Department as containing important information, which could include systems which provide a customer presence, process orders, or facilitate communication. At a minimum the following are expected:

Provide forensic services to investigate real or perceived breaches of the Department network and/or information system. Forensic imaging and preservation of chain of custody, log analysis, file system analysis, operating system configuration and vulnerability analysis, web server and application analysis, network application vulnerability analysis, timeline analysis and residual threat analysis.

4.5.2 Scope

To retain a Vendor to perform forensic services as required. To ensure the requirements established by the acquiring bank are met. Provide a detailed report / impact assessment upon conclusion of engagement and make recommendations for remediation to bring the Department into compliance. An executive level out briefing will also be delivered to summarize findings and recommendations.

Vendor must be a qualified forensic expert that is a Visa-approved Qualified Incident Response Assessor (QIRA).

All work performed must be in accordance with acquiring bank and Visa USA, Inc. specified guidance for forensic services.

All deliverables must be in accordance with the acquiring bank and Visa USA, Inc. specified requirements for the reporting of security breaches.

4.5.3 Work Approach

Vendor must specify its project management and technical approach for this engagement.

4.5.4 Deliverables

Deliverables and documentation to be produced by Vendor:

After active testing has concluded, the Vendor will provide a detailed report that outlines impact assessment and provide remediation recommendations. Screen shots and log excerpts may be included, when applicable. An out briefing to summarize findings and recommendations is expected. This can be delivered in PowerPoint format.

Documentation to be produced by the Department and Department obligations:

The Department will make available all necessary personnel to Vendor during the period of performance.

The Department understands that the following must be provided to Vendor, upon suspicion of a security breach, the Department will immediately contact Vendor to schedule commencement of this engagement:

Addresses of, and appropriate access to networked devices and systems to within the scope of the assessment, a list of appropriate contact personnel with “after hours” emergency contacts numbers, access to the network and all affected systems, access to system configuration documentation and

The Department personnel (administrators) required to answer questions and complete investigations.

4.6 Business Impact Analysis (BIA)

4.6.1 Objective

The Department is seeking a qualified Vendor to conduct a Business Impact Analysis.

4.6.2 Scope

The Vendor shall perform an on-site assessment of the business units within the Division of Toll Operations, as described below, and identify cumulative financial impacts over time as well as intangible (brand image, etc.) impacts of an extended interruption of operations.

SunPass Operations: This includes the SunPass Call Center in Boca Raton, FL and Orlando, FL (Southland), as well as the, SunPass operations, mail processing, payment processing, shipping, training, QA, and Vehicle Enforcement System Operations (VES).

SunPass accounting and Traffic and Revenue Audit Center: This includes the Toll Plaza Audit (Ticket and Barrier) and Bank Audit (Ticket and Barrier).

SunWatch operations, desktop end-user environments, tolls applications located and managed with the TDC and the connections to plazas, and the backup/testing facility at the Orlando Data Center (ODC).

4.6.3 Work Approach

The Vendor must comply with the following requirements:

The Vendor shall include at least one (1) member with a finance background who has the ability to guide and assist the business units in the process of identifying the financial impacts on their staff.

Provide the methodology for evaluating the intangible impacts; such as, brand image, customer satisfaction.

Provide detailed description of metrics and formulas that will be used to establish the impacts and to rank the results.

Provide sample questionnaire/survey that will be used during business unit interviews.

4.6.4 Deliverable

The BIA report will identify the criticality level of each business unit along with recovery time objectives for the unit and its associated technology, recovery point objectives for the associated critical data, supporting technology required to sustain operations over identified time frames.

4.6.5 Exclusions

Applications on desktop pcs and the toll plaza facilities/operations.

5. SUBLETTING OR ASSIGNING OF WORK

The Vendor shall not sublet, assign or transfer any work under this Agreement, without written consent by the Department. Any and all subvendors are required to be qualified and certified in accordance with the requirements herein, all federal, state and local regulations, and approved by the Department. Subletting of work shall not relieve the Vendor of their respective liabilities. The Department recognizes a subvendor only in the capacity of an employee or agent of the Vendor.

Subvendors providing portions of the services under the Contract shall meet all project delivery requirements and provide the same level of service required of the Vendor. If the Vendor uses a subvendor, the following conditions apply under the listed circumstances:

5.1 Any subcontract rendered by individuals or organizations not a part of the Vendor's firm shall not be executed without prior authorization and written approval from the Department.

5.2 The Department retains the right to verify a sub-vendor's background and make a determination to accept or reject the proposed subvendors. The approval or disapproval of a sub-vendor is at the sole discretion of the Department.

5.3 The Vendor shall be solely responsible and accountable for the completion of all work for which the Vendor has subcontracted. The Department reserves the right to authorize the removal of any subvendor's employee deemed as unsatisfactory by the Department.

5.3.1 The Department will consider the Vendor to be the sole point of contact with regard to items subcontracted.

6. COST

- 6.1 Cost must include travel expenses in accordance with the State of Florida expense policy currently in effect, if applicable.
- 6.2 Cost for the forensic security services includes one (1) Senior Subject Matter Expert (SSME) full-time equivalent to thirty (30) hours annually. Addition hours billed (as required) at stated fixed rate.

7. SCHEDULE

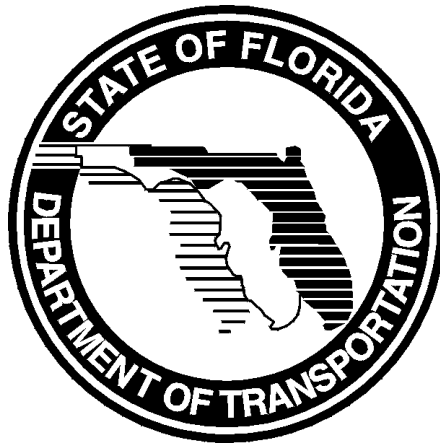
- 7.1 Vendor must provide a schedule of activities for the engagement.
- 7.2 Vendor must specify the task to be performed by the Department technical staff prior to and during this engagement.

8. WARRANTY INDEMNITY

Vendor warrants that it has full power and authority to grant the rights granted by this Agreement to the Department, and that neither the performance of this Agreement by Vendor, nor the license or other rights granted to the Department hereunder, or the use by the Department of any software, will in any way violate any non-disclosure agreement or constitute infringement or other violation of any copyright, trade secret, trademark, service mark, invention, proprietary information, or other rights of any third party. Vendor agrees to indemnify, defend, and hold harmless the Department, its officers, employees, and agents from and against any and all claims, proceedings, liabilities, losses, damages, costs, and expenses, including without limitation, reasonable attorneys' fees, arising out of or in connection with any claim that the software infringes upon or otherwise violates any copyright, trade secret, trademark, service mark, invention, proprietary information, or other rights of any third party. Vendor also agrees that if the Department's use of or license to the software becomes the subject of an infringement claim, Vendor shall, at its sole expense, either procure the right for the Department to continue to use and license the software or modify or replace the software or affected component thereof with another item of comparable quality and performance capabilities so as to become non-infringing.

9. DURATION OF CONTRACT

Work shall commence upon the start date identified in the written Notice to Proceed from the Project Manager and shall be for three (3) years from the date of notification. This agreement may be renewed for up to three (3) additional years. Renewals shall be contingent upon satisfactory performance evaluation by the Department and subject to the availability of funds. Any renewals or extensions shall be in writing and executed by both parties, and shall be subject to the same terms and conditions set forth in this Agreement.



ATTACHMENTS

RFP-DOT- 09/10-8001-KB

PAYMENT CARD INDUSTRY (PCI) SERVICES

FPI No. 423249-1-32-01

**State of Florida
Department of Transportation
Florida's Turnpike Enterprise**

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement, (hereinafter the "Agreement") is made and entered in this _____ day of _____, 2009, by and between _____ with its principle place of business at _____, hereinafter "Undersigned", and the State of Florida, Department of Transportation, Turnpike Enterprise, with headquarters located at Florida's Turnpike, Turkey Lake Service Plaza, Milepost 263, Building 5315, Post Office Box 613069, Ocoee, Florida 34761, hereinafter the "Disclosing Party".

Whereas, The parties to this Agreement recognize and acknowledge that it may be necessary or desirable to exchange certain information for the required services outlined in the RFP to be met, in this case IP Addresses, Access to systems and databases that contains PII, credit card information, application code and scripts.

Now, therefore, In consideration of the delivery to a Proposer, the "Undersigned," by the State of Florida, Department of Transportation (FDOT), as the "Disclosing Party", of certain confidential and proprietary information, collectively, the "Proprietary Information," and the mutual covenants and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Undersigned hereby agrees to hold all such Proprietary Information in confidence and not to use, except for the purpose(s) described herein, or disclose the same to third parties except with the prior written consent of the Disclosing Party.

Proprietary Information includes all information furnished by the Disclosing Party to the Undersigned hereunder, or to any agent or employee of the Undersigned, directly or indirectly, which information the Disclosing Party regards as proprietary and wishes to protect from unauthorized disclosure, whether such information is transferred orally, visually, electronically or by any other means.

The Undersigned shall be deemed to have met its obligations hereunder if it treats the Proprietary Information with the same degree of care with which the Undersigned treats its own proprietary and confidential information, or reasonable care under the circumstances, whichever is more stringent. The Undersigned's obligations do not extend to Proprietary Information which:

1. is or becomes part of the public domain through no violation of this Agreement by the Undersigned or its employees or agents;
2. is in the possession of the Undersigned prior to disclosure thereof by the Disclosing Party;
3. was independently developed by the Undersigned;
4. is disclosed pursuant to a court order; or
5. is or may be obtained by the Undersigned from an independent third party or source without an obligation of confidentiality.

The Undersigned agrees it will use the Proprietary Information for the benefit of the Disclosing Party only and the purposes described herein only and shall not disclose it to anyone other than its agents or employees who have a need to know for the benefit of the Disclosing Party. The Undersigned also agrees to have its subcontractors execute this Non-Disclosure Agreement prior to receiving any of the Disclosing Party's proprietary information.

All Proprietary Information delivered by the Disclosing Party to the Undersigned pursuant to this Agreement shall be and remain the property of the Disclosing Party, and the Undersigned shall, within a mutually agreed upon time frame, return all such information when requested to do so by the Disclosing Party.

The Undersigned also agrees to have its subcontractors execute this Non-Disclosure Agreement prior to receiving any of Disclosing Party's proprietary information.

In those cases where the Proprietary Information constitutes a trade secret as defined by applicable law, the Proprietary Information shall be afforded all of the protections available to trade secrets under applicable law.

The Undersigned shall indemnify, defend and save harmless the Disclosing Party from and against any and all claims, demands, actions or causes of action that are asserted against the Disclosing Party which arise out of or are related to use of the Proprietary Information or a breach of confidentiality as contemplated within this Agreement.

IN PROVIDING ANY DATA HEREUNDER, THE DISCLOSING PARTY MAKES NO REPRESENTATIONS OR WARRANTIES, EITHER EXPRESS OR IMPLIED, AS TO ADEQUACY, SUFFICIENCY, OR FREEDOM FROM DEFECT OF ANY KIND, INCLUDING FREEDOM FROM ANY PATENT INFRINGEMENT THAT MAY RESULT FROM THE USE OF SUCH DATA.

The Undersigned acknowledges that unauthorized disclosure of the Proprietary Information will diminish substantially the value of the Proprietary Information. If the Undersigned violates the provisions of this Agreement, the Disclosing Party shall be entitled to obtain equitable relief to protect its interests herein, including, but not limited to, injunctive relief, as well as monetary damages.

This Agreement contains the entire agreement relative to the protection of information exchanged in connection with the Proprietary Information and supersedes any prior or collateral understanding among the parties hereto. This Agreement shall apply in lieu of and notwithstanding any specific legends or statement associated with any particular information. This Agreement shall not be modified or amended, except in a written instrument executed by authorized representatives of the parties hereto.

Nothing in this Agreement, or the disclosure of any information by either party, shall be deemed by implication or otherwise to convey to disclose any rights, title, interest, or license under any patents, patent applications, or inventions of any party.

Nothing contained in this Agreement is intended to or shall grant to any party the right to make commitments of any kind for or on behalf of any other party without the prior written consent of that other party.

The validity, construction and performance of this Agreement shall be governed by, construed and interpreted in accordance with the laws of the State of Florida. If any covenant or provision of this Agreement is determined by a court of competent jurisdiction to be void, invalid or unenforceable in whole or in part, then such void, invalid or unenforceable covenant or provision shall be adjusted so as to best reflect the intent of the parties to the maximum extent possible, or deleted from this Agreement and shall not effect or impair the enforceability or validity of any other covenant or provision of this Agreement or any part thereof.

This Agreement may not be sold, assigned or otherwise transferred by a party in whole or in part without the express prior written consent of the other party. This Agreement shall benefit and be binding upon the successors, assigns and representatives of the parties hereto.

Any representations, rights and obligations under this Agreement that by their nature are continuous or extend beyond the terms of this Agreement shall survive any expiration or termination of this Agreement and shall remain in effect until complete performance thereof has occurred. The failure of either party to enforce any right accruing under this Agreement shall not be construed as a waiver of a subsequent right of such party to enforce the same or any other right, term or condition.

Each individual executing this Agreement on behalf of a party personally warrants that he or she is authorized to enter into and execute this Agreement on behalf of such party and that this Agreement is binding on that party and on the individual executing this Agreement.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed on the date stipulated below:

STATE OF FLORIDA
DEPARTMENT OF TRANSPORTATION

DISCLOSING PARTY

AUTHORIZED SIGNATURE

DATE

Christopher L Warren, Deputy Executive Director –
Florida Turnpike Enterprise

PRINTED (TYPED) SIGNATURE & TITLE

UNDERSIGNED (PROPOSER NAME)

AUTHORIZED SIGNATURE

DATE

PRINTED (TYPED) SIGNATURE & TITLE



Payment Card Industry (PCI) Data Security Standard

Requirements and Security Assessment Procedures

Version 1.2

October 2008

Table of Contents

Introduction and PCI Data Security Standard Overview	3
PCI DSS Applicability Information	4
Scope of Assessment for Compliance with PCI DSS Requirements.....	5
<i>Network Segmentation.....</i>	<i>5</i>
<i>Wireless</i>	<i>6</i>
<i>Third Parties/Outsourcing</i>	<i>6</i>
<i>Sampling of Business Facilities and System Components.....</i>	<i>6</i>
<i>Compensating Controls</i>	<i>7</i>
Instructions and Content for Report on Compliance	8
<i>Report Content and Format</i>	<i>8</i>
<i>Revalidation of Open Items.....</i>	<i>11</i>
<i>PCI DSS Compliance – Completion Steps.....</i>	<i>11</i>
Detailed PCI DSS Requirements and Security Assessment Procedures.....	12
Build and Maintain a Secure Network	13
<i>Requirement 1: Install and maintain a firewall configuration to protect cardholder data</i>	<i>13</i>
<i>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters</i>	<i>17</i>
Protect Cardholder Data	20
<i>Requirement 3: Protect stored cardholder data.....</i>	<i>20</i>
<i>Requirement 4: Encrypt transmission of cardholder data across open, public networks.....</i>	<i>26</i>
Maintain a Vulnerability Management Program	28
<i>Requirement 5: Use and regularly update anti-virus software or programs.....</i>	<i>28</i>
<i>Requirement 6: Develop and maintain secure systems and applications</i>	<i>29</i>
Implement Strong Access Control Measures	35
<i>Requirement 7: Restrict access to cardholder data by business need to know.....</i>	<i>35</i>
<i>Requirement 8: Assign a unique ID to each person with computer access.</i>	<i>37</i>
<i>Requirement 9: Restrict physical access to cardholder data.....</i>	<i>42</i>
Regularly Monitor and Test Networks	46
<i>Requirement 10: Track and monitor all access to network resources and cardholder data.</i>	<i>46</i>
<i>Requirement 11: Regularly test security systems and processes.....</i>	<i>49</i>
Maintain an Information Security Policy	52
<i>Requirement 12: Maintain a policy that addresses information security for employees and contractors.....</i>	<i>52</i>
Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers	59
Appendix B: Compensating Controls.....	61
Appendix C: Compensating Controls Worksheet.....	62

Appendix D: Attestation of Compliance – Merchants.....	64
Appendix E: Attestation of Compliance – Service Providers.....	68
Appendix F: PCI DSS Reviews — Scoping and Selecting Samples	72

Introduction and PCI Data Security Standard Overview

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. This document, *PCI Data Security Standard Requirements and Security Assessment Procedures*, uses as its foundation the 12 PCI DSS requirements, and combines them with corresponding testing procedures into a security assessment tool. It is designed for use by assessors conducting onsite reviews for merchants and service providers who must validate compliance with the PCI DSS. Below is a high-level overview of the 12 PCI DSS requirements. The next several pages provide background about preparing for, conducting, and reporting a PCI DSS assessment, whereas the detailed PCI DSS requirements begin on page 13.

PCI Data Security Standard – High-Level Overview

Build and Maintain a Secure Network

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security

PCI DSS Applicability Information

The following table illustrates commonly used elements of cardholder and sensitive authentication data; whether storage of each data element is permitted or prohibited; and whether each data element must be protected. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name ¹	Yes	Yes ¹	No
	Service Code ¹	Yes	Yes ¹	No
	Expiration Date ¹	Yes	Yes ¹	No
Sensitive Authentication Data ²	Full Magnetic Stripe Data ³	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

¹ These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

² Sensitive authentication data must not be stored after authorization (even if encrypted).

³ Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.

Scope of Assessment for Compliance with PCI DSS Requirements

The PCI DSS security requirements apply to all system components. "System components" are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications.

Network Segmentation

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement. However, it is recommended as a method that may reduce:

- The scope of the PCI DSS assessment
- The cost of the PCI DSS assessment
- The cost and difficulty of implementing and maintaining PCI DSS controls
- The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)

Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment. Network segmentation can be achieved through internal network firewalls, routers with strong access control lists or other technology that restricts access to a particular segment of a network.

An important prerequisite to reduce the scope of the cardholder data environment is a clear understanding of business needs and processes related to the storage, processing or transmission of cardholder data. Restricting cardholder data to as few locations as possible by elimination of unnecessary data, and consolidation of necessary data, may require reengineering of long-standing business practices.

Documenting cardholder data flows via a dataflow diagram helps fully understand all cardholder data flows and ensures that any network segmentation is effective at isolating the cardholder data environment.

If network segmentation is in place and will be used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment. At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not. However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon such things as a given network's configuration, the technologies deployed, and other controls that may be implemented.

Appendix F: PCI DSS Reviews – Scoping and Selecting Samples provides more information on the effect of scoping during a PCI DSS assessment.

Wireless

If wireless technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, “line-busting”), or if a wireless local area network (LAN) is connected to or part of the cardholder data environment (for example, not clearly separated by a firewall), the PCI DSS requirements and testing procedures for wireless environments apply and must be performed as well (for example, Requirements 1.2.3, 2.1.1, and 4.1.1). Before wireless technology is implemented, a company should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.

Third Parties/Outsourcing

For service providers required to undergo an annual onsite assessment, compliance validation must be performed on all system components where cardholder data is stored, processed, or transmitted.

A service provider or merchant may use a third-party provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.

For those entities that outsource storage, processing, or transmission of cardholder data to third-party service providers, the Report on Compliance (ROC) must document the role of each service provider, clearly identifying which requirements apply to the reviewed entity and which apply to the service provider. There are two options for third-party service providers to validate compliance: 1) They can undergo a PCI DSS assessment on their own and provide evidence to their customers to demonstrate their compliance, or 2) If they do not undergo their own PCI DSS assessment, they will need to have their services reviewed during the course of each of their customer's PCI DSS assessments. See the bullet beginning “For managed service provider (MSP) reviews” under Part 3 in the “Instructions and Content for Report on Compliance” section below for more information.

Additionally, merchants and service providers must manage and monitor the PCI DSS compliance of all associated third parties with access to cardholder data. *Refer to Requirement 12.8 in this document for details.*

Sampling of Business Facilities and System Components

The assessor may select representative samples of business facilities and system components in order to assess PCI DSS requirements. These samples must include both business facilities and system components, must be a representative selection of all of the types and locations of business facilities as well as types of system components, and must be sufficiently large to provide the assessor with assurance that controls are implemented as expected.

Examples of business facilities include corporate offices, stores, franchise merchants, and business facilities in different locations. Sampling should include system components for each business facility. For example, for each business facility, include a variety of operating systems, functions, and applications that are applicable to the area under review. Within each business facility, the reviewer could choose Sun servers running Apache WWW, Windows servers running Oracle, mainframe systems running legacy card processing applications, data transfer servers running HP-UX, and Linux Servers running MYSQL. If all applications run from a single OS (for example, Windows or Sun), then the sample

should still include a variety of applications (for example, database servers, web servers, data transfer servers). (See *Appendix F: PCI DSS Reviews – Scoping and Sampling*.)

When selecting samples of business facilities and system components, assessors should consider the following:

- If there are standard, required PCI DSS processes in place that each facility must follow, the sample can be smaller than is necessary if there are no standard processes, to provide reasonable assurance that each facility is configured per the standard process.
- If there is more than one type of standard process in place (for example, for different types of system components or facilities), then the sample must be large enough to include system components or facilities secured with each type of process.
- If there are no standard PCI DSS processes in place and each facility is responsible for their processes, then sample size must be larger to be assured that each facility understands and implements PCI DSS requirements appropriately.

Please also refer to Appendix F: PCI DSS Reviews – Scoping and Selecting Samples.

Compensating Controls

On an annual basis, any compensating controls must be documented, reviewed and validated by the assessor and included with the Report on Compliance submission, per *Appendix B: Compensating Controls* and *Appendix C: Compensating Controls Worksheet*.

For each and every compensating control, the Compensating Controls Worksheet (Appendix C) **must** be completed. Additionally, compensating control results should be documented in the ROC in the corresponding PCI DSS requirement section.

See the above-mentioned Appendices B and C for more details on “compensating controls.”

Instructions and Content for Report on Compliance

This document must be used as the template for creating the *Report on Compliance*. The assessed entity should follow each payment brand's respective reporting requirements to ensure each payment brand acknowledges the entity's compliance status. Contact each payment brand to determine reporting requirements and instructions.

Report Content and Format

Follow these instructions for report content and format when completing a Report on Compliance:

1. Executive Summary

Include the following:

- Describe the entity's payment card business, including:
 - Their business role with payment cards, which is how and why they store, process, and/or transmit cardholder data
Note: This is not intended to be a cut-and-paste from the entity's web site, but should be a tailored description that shows the assessor understands payment and the entity's role.
 - How they process payment (directly, indirectly, etc.)
 - What types of payment channels they serve, such as card-not-present, (for example, mail-order-telephone-order (MOTO), e-Commerce), or card-present
 - Any entities that they connect to for payment transmission or processing, including processor relationships
- A high-level network diagram (either obtained from the entity or created by assessor) of the entity's networking topography that includes:
 - Connections into and out of the network
 - Critical components within the cardholder data environment, including POS devices, systems, databases, and web servers, as applicable
 - Other necessary payment components, as applicable

2. Description of Scope of Work and Approach Taken

Describe the scope, per the Scope of Assessment section of this document, including the following:

- Environment on which assessment focused (for example, client's Internet access points, internal corporate network, processing connections)
- If network segmentation is in place and was used to reduce scope of the PCI DSS review, briefly explain that segmentation and how assessor validated the effectiveness of the segmentation
- Document and justify sampling used for both entities (stores, facilities, etc.) and system components selected, including:
 - Total population
 - Number sampled
 - Rationale for sample selected
 - Why sample size is sufficient to allow assessor to place reasonable reliance that controls reviewed represent controls in place throughout entity
 - Describe any locations or environments that store, process, or transmit cardholder data that were EXCLUDED from the scope of the review, and why these locations/environments were excluded
- List any wholly-owned entities that require compliance with the PCI DSS, and whether they are reviewed separately or as part of this assessment
- List any International entities that require compliance with the PCI DSS, and whether they are reviewed separately or as part of this assessment
- List any wireless LANs and/or wireless payment applications (for example, POS terminals) that are connected to, or could impact the security of the cardholder data environment, and describe security in place for these wireless environments
- The version of the PCI DSS Requirements and Security Assessment Procedures document used to conduct the assessment
- Timeframe of assessment

3. Details about Reviewed Environment

Include the following details in this section:

- A diagram of each piece of the communication link, including LAN, WAN or Internet
- Description of cardholder data environment, for example:
 - Document transmission and processing of cardholder data, including authorization, capture, settlement, chargeback and other flows as applicable

- List of files and tables that store cardholder data, supported by an inventory created (or obtained from the client) and retained by the assessor in the work papers. This inventory should include, for each cardholder data store (file, table, etc.):
 - List all of the elements of stored cardholder data
 - How data is secured
 - How access to data stores are logged
- List of hardware and critical software in use in the cardholder data environment, along with description of function/use for each
- List of service providers and other entities with which the company shares cardholder data (Note: these entities are subject to PCI DSS Requirement 12.8)
- List of third-party payment application products and versions numbers in use, including whether each payment application has been validated according to PA-DSS. Even if a payment application has been PA-DSS validated, the assessor still needs to verify that the application has been implemented in a PCI DSS compliant manner and environment, and according to the payment application vendor's PA-DSS *Implementation Guide*. *Note: It is not a PCI DSS requirement to use PA-DSS validated applications. Please consult with each payment brand individually to understand their PA-DSS compliance requirements.*
- List of individuals interviewed and their titles
- List of documentation reviewed
- For managed service provider (MSP) reviews, the assessor must clearly identify which requirements in this document apply to the MSP (and are included in the review), and which are not included in the review and are the responsibility of the MSP's customers to include in their reviews. Include information about which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans, and which IP addresses are the responsibility of the MSP's customers to include in their own quarterly scans.

4. Contact Information and Report Date

Include:

- Contact information for merchant or service provider and assessor
- Date of report

5. Quarterly Scan Results

- Summarize the four most recent quarterly scan results in the Executive Summary as well as in comments at Requirement 11.2

Note: It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning going forward, and 3) any vulnerabilities noted in the initial scan have been corrected as shown in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.

- Scan must cover all externally accessible (Internet-facing) IP addresses in existence at the entity, in accordance with the *PCI DSS Security Scanning Procedures*

6. Findings and Observations

- Summarize in the Executive Summary any findings that may not fit into the standard Report on Compliance template format.
- All assessors *must* use the Detailed PCI DSS Requirements and Security Assessment Procedures template to provide detailed report descriptions and findings on each requirement and sub-requirement.
- The assessor *must* review and document any compensating controls considered to conclude that a control is in place.

See Compensating Controls section above and Appendices B and C for more details on “compensating controls.”

Revalidation of Open Items

A “controls in place” report is required to verify compliance. The report is considered non-compliant if it contains “open items,” or items that will be finished at a future date. The merchant/service provider must address these items before validation is completed. After these items are addressed by the merchant/service provider, the assessor will then reassess to validate that the remediation occurred and that all requirements are satisfied. After revalidation, the assessor will issue a new Report on Compliance, verifying that the cardholder data environment is fully compliant, and submit it consistent with instructions (see below).

PCI DSS Compliance – Completion Steps

1. Complete the Report on Compliance (ROC) according to the section above entitled “Instructions and Content for Report on Compliance.”
2. Ensure passing vulnerability scan(s) have been completed by a PCI SSC Approved Scanning Vendor (ASV), and obtain evidence of passing scan(s) from the ASV.
3. Complete the Attestation of Compliance, for either Service Providers or Merchants as applicable, in its entirety. See Appendices D and E for Attestations of Compliance.
4. Submit the ROC, evidence of a passing scan, and the Attestation of Compliance, along with any other requested documentation, to the acquirer (for merchants) or to the payment brand or other requester (for service providers).

Detailed PCI DSS Requirements and Security Assessment Procedures

For the *PCI DSS Requirements and Security Assessment Procedures*, the following defines the table column headings:

- **PCI DSS Requirements** – This column defines the Data Security Standard and lists requirements to achieve PCI DSS compliance; compliance will be validated against these requirements.
- **Testing Procedures** – This column shows processes to be followed by the assessor to validate that PCI DSS requirements are “in place”
- **In Place** – This column must be used by the assessor to provide a brief description of controls found in place, including those controls found to be in place as a result of compensating controls. (Note: that this column must *not* be used for items that are not yet in place or for open items to be completed at a future date.)
- **Not in Place** – This column must be used by the assessor to provide a brief description controls that are not in place. Note that a non-compliant report should not be submitted to a payment brand or acquirer unless specifically requested. See Appendix D and Appendix E: Attestations of Compliance for further instructions on non-compliant reports.
- **Target Date/Comments** – For those controls “Not In Place” the assessor may include a target date that the merchant or service provider expects to have controls “In Place”. Any additional notes or comments may be included here as well.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed between a company's network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1 Establish firewall and router configuration standards that include the following:	1.1 Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	1.1.1 Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.			
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	1.1.2.a Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.			
	1.1.2.b Verify that the diagram is kept current.			
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	1.1.3 Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. Verify that the current network diagram is consistent with the firewall configuration standards.			
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	1.1.4 Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	1.1.5.a Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.			
	1.1.5.b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.			
1.1.6 Requirement to review firewall and router rule sets at least every six months	1.1.6.a Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.			
	1.1.6.b Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.			
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	1.2 Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:			
<i>Note: An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity’s ability to control or manage.</i>				
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	1.2.1.a Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.			
	1.2.1.b Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement.			
1.2.2 Secure and synchronize router configuration files.	1.2.2 Verify that router configuration files are secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	1.2.3 Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.			
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	1.3 Examine firewall and router configurations, as detailed below, to determine that there is no direct access between the Internet and system components, including the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment.			
1.3.1 Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	1.3.1 Verify that a DMZ is implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.			
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	1.3.2 Verify that inbound Internet traffic is limited to IP addresses within the DMZ.			
1.3.3 Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.	1.3.3 Verify there is no direct route inbound or outbound for traffic between the Internet and the cardholder data environment.			
1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.	1.3.4 Verify that internal addresses cannot pass from the Internet into the DMZ.			
1.3.5 Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.	1.3.5 Verify that outbound traffic from the cardholder data environment to the Internet can only access IP addresses within the DMZ.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	1.3.6 Verify that the firewall performs stateful inspection (dynamic packet filtering). [Only established connections should be allowed in, and only if they are associated with a previously established session (run a port scanner on all TCP ports with "syn reset" or "syn ack" bits set—a response means packets are allowed through even if they are not part of a previously established session).]			
1.3.7 Place the database in an internal network zone, segregated from the DMZ.	1.3.7 Verify that the database is on an internal network zone, segregated from the DMZ.			
1.3.8 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).	1.3.8 For the sample of firewall and router components, verify that NAT or other technology using RFC 1918 address space is used to restrict broadcast of IP addresses from the internal network to the Internet (IP masquerading).			
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	1.4.a Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active.			
	1.4.b Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by mobile computer users.			

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.1 Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	2.1 Choose a sample of system components, critical servers, and wireless access points, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)			
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	2.1.1 Verify the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (for example, AES): ▪ Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions ▪ Default SNMP community strings on wireless devices were changed ▪ Default passwords/passphrases on access points were changed ▪ Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2) ▪ Other security-related wireless vendor defaults, if applicable			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	2.2.a Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards—for example, SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).			
	2.2.b Verify that system configuration standards include each item below (at 2.2.1 – 2.2.4).			
	2.2.c Verify that system configuration standards are applied when new systems are configured.			
2.2.1 Implement only one primary function per server.	2.2.1 For a sample of system components, verify that only one primary function is implemented per server. For example, web servers, database servers, and DNS should be implemented on separate servers.			
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).	2.2.2 For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that unnecessary or insecure services or protocols are not enabled, or are justified and documented as to appropriate use of the service. For example, FTP is not used, or is encrypted via SSH or other technology.			
2.2.3 Configure system security parameters to prevent misuse.	2.2.3.a Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.			
	2.2.3.b Verify that common security parameter settings are included in the system configuration standards.			
	2.2.3.c For a sample of system components, verify that common security parameters are set appropriately.			
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	2.2.4 For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. Verify enabled functions are documented and support secure configuration, and that only documented functionality is present on the sampled machines.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	2.3 For a sample of system components, verify that non-console administrative access is encrypted by: ▪ Observing an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested; ▪ Reviewing services and parameter files on systems to determine that Telnet and other remote log-in commands are not available for use internally; and ▪ Verifying that administrator access to the web-based management interfaces is encrypted with strong cryptography.			
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in <i>Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers</i> .	2.4 Perform testing procedures A.1.1 through A.1.4 detailed in <i>Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers</i> for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.			

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

Please refer to the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of “strong cryptography” and other PCI DSS terms.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	3.1 Obtain and examine the company policies and procedures for data retention and disposal, and perform the following - Verify that policies and procedures include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons) - Verify that policies and procedures include provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data - Verify that policies and procedures include coverage for all storage of cardholder data - Verify that policies and procedures include a programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, requirements for a review, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	3.2 If sensitive authentication data is received and deleted, obtain and review the processes for deleting the data to verify that the data is unrecoverable. For each item of sensitive authentication data below, perform the following steps:			
3.2.1 Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. <i>Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:</i> ▪ The cardholder's name, ▪ Primary account number (PAN), ▪ Expiration date, and ▪ Service code <i>To minimize risk, store only these data elements as needed for business.</i> <i>Note: See PCI DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i>	3.2.1 For a sample of system components, examine the following and verify that the full contents of any track from the magnetic stripe on the back of card are not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.2.2 Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. <i>Note: See PCI DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i>	3.2.2 For a sample of system components, verify that the three-digit or four-digit card-verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents			
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	3.2.3 For a sample of system components, examine the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents			
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). <i>Notes:</i> ▪ <i>This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.</i> ▪ <i>This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.</i>	3.3 Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches: - One-way hashes based on strong cryptography - Truncation - Index tokens and pads (pads must be securely stored) - Strong cryptography with associated key-management processes and procedures The MINIMUM account information that must be rendered unreadable is the PAN. <i>Notes:</i> <i>If for some reason, a company is unable render the PAN unreadable, refer to Appendix B: Compensating Controls.</i> <i>“Strong cryptography” is defined in the PCI DSS Glossary of Terms, Abbreviations, and Acronyms.</i>	3.4.a Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using one of the following methods: - One-way hashes based on strong cryptography - Truncation - Index tokens and pads, with the pads being securely stored - Strong cryptography, with associated key-management processes and procedures			
	3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).			
	3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.			
	3.4.d Examine a sample of audit logs to confirm that the PAN is sanitized or removed from the logs.			
	3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must			
	3.4.1.a If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).			
	3.4.1.b Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
not be tied to user accounts.	3.4.1.c Verify that cardholder data on removable media is encrypted wherever stored. <i>Note: Disk encryption often cannot encrypt removable media, so data stored on this media will need to be encrypted separately.</i>			
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:	3.5 Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:			
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	3.5.1 Examine user access lists to verify that access to keys is restricted to very few custodians.			
3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	3.5.2 Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys.			
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	3.6.a Verify the existence of key-management procedures for keys used for encryption of cardholder data. <i>Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.</i>			
	3.6.b For service providers only: If the service provider shares keys with their customers for transmission of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely store and change customer's keys (used to transmit data between customer and service provider).			
	3.6.c Examine the key-management procedures and perform the following:			
3.6.1 Generation of strong cryptographic keys	3.6.1 Verify that key-management procedures are implemented to require the generation of strong keys.			
3.6.2 Secure cryptographic key distribution	3.6.2 Verify that key-management procedures are implemented to require secure key distribution.			
3.6.3 Secure cryptographic key storage	3.6.3 Verify that key-management procedures are implemented to require secure key storage.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.6.4 Periodic cryptographic key changes - As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically - At least annually	3.6.4 Verify that key-management procedures are implemented to require periodic key changes at least annually.			
3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys	3.6.5.a Verify that key-management procedures are implemented to require the retirement of old keys (for example: archiving, destruction, and revocation as applicable).			
	3.6.5.b Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.			
3.6.6 Split knowledge and establishment of dual control of cryptographic keys	3.6.6 Verify that key-management procedures are implemented to require split knowledge and dual control of keys (for example, requiring two or three people, each knowing only their own part of the key, to reconstruct the whole key).			
3.6.7 Prevention of unauthorized substitution of cryptographic keys	3.6.7 Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.			
3.6.8 Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	3.6.8 Verify that key-management procedures are implemented to require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.			

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. <i>Examples of open, public networks that are in scope of the PCI DSS are:</i> ▪ The Internet, ▪ Wireless technologies, ▪ Global System for Mobile communications (GSM), and ▪ General Packet Radio Service (GPRS).	4.1.a Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks ▪ Verify that strong encryption is used during data transmission ▪ For SSL implementations: – Verify that the server supports the latest patched versions. – Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). – Verify that no cardholder data is required when HTTPS does not appear in the URL. ▪ Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit. ▪ Verify that only trusted SSL/TLS keys/certificates are accepted. ▪ Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. - For new wireless implementations, it is prohibited to implement WEP after March 31, 2009. - For current wireless implementations, it is prohibited to use WEP after June 30, 2010.	4.1.1 For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.			
4.2 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).	4.2.a Verify that strong cryptography is used whenever cardholder data is sent via end-user messaging technologies.			
	4.2.b Verify the existence of a policy stating that unencrypted PANs are not to be sent via end-user messaging technologies.			

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters the network during many business approved activities including employees’ e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	5.1 For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.			
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	5.1.1 For a sample of system components, verify that all anti-virus programs detect, remove, and protect against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits).			
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	5.2 Verify that all anti-virus software is current, actively running, and capable of generating logs by performing the following:			
	5.2.a Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.			
	5.2.b Verify that the master installation of the software is enabled for automatic updates and periodic scans.			
	5.2.c For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled.			
	5.2.d For a sample of system components, verify that antivirus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7			

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release. <i>Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.</i>	6.1.a For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.			
	6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.			
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	6.2.a Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities.			
	6.2.b Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2.2 as new vulnerability issues are found.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.3 Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle. These processes must include the following:	6.3.a Obtain and examine written software development processes to verify that the processes are based on industry standards, security is included throughout the life cycle, and software applications are developed in accordance with PCI DSS.			
	6.3.b From an examination of written software development processes, interviews of software developers, and examination of relevant data (network configuration documentation, production and test data, etc.), verify that:			
6.3.1 Testing of all security patches, and system and software configuration changes before deployment, including but not limited to the following:	6.3.1 All changes (including patches) are tested before being deployed into production.			
6.3.1.1 Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)	6.3.1.1 Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)			
6.3.1.2 Validation of proper error handling	6.3.1.2 Validation of proper error handling			
6.3.1.3 Validation of secure cryptographic storage	6.3.1.3 Validation of secure cryptographic storage			
6.3.1.4 Validation of secure communications	6.3.1.4 Validation of secure communications			
6.3.1.5 Validation of proper role-based access control (RBAC)	6.3.1.5 Validation of proper role-based access control (RBAC)			
6.3.2 Separate development/test and production environments	6.3.2 The development/test environments are separate from the production environment, with access control in place to enforce the separation.			
6.3.3 Separation of duties between development/test and production environments	6.3.3 There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.			
6.3.4 Production data (live PANs) are not used for testing or development	6.3.4 Production data (live PANs) are not used for testing and development, or are sanitized before use.			
6.3.5 Removal of test data and accounts before production systems become active	6.3.5 Test data and accounts are removed before a production system becomes active.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.3.6 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	6.3.6 Custom application accounts, user IDs and/or passwords are removed before system goes into production or is released to customers.			
6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability <i>Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.</i>	6.3.7.a Obtain and review policies to confirm all custom application code changes for <i>internal applications</i> must be reviewed (either using manual or automated processes), as follows: - Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. - Appropriate corrections are implemented prior to release. - Code review results are reviewed and approved by management prior to release.			
	6.3.7.b Obtain and review policies to confirm that all custom application code changes for <i>web applications</i> must be reviewed (using either manual or automated processes) as follows: - Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. - Code reviews ensure code is developed according to secure coding guidelines such as the <i>Open Web Security Project Guide</i> (see PCI DSS Requirement 6.5). - Appropriate corrections are implemented prior to release. - Code review results are reviewed and approved by management prior to release.			
	6.3.7.c Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.7a and 6.3.7b above.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.4 Follow change control procedures for all changes to system components. The procedures must include the following:	6.4.a Obtain and examine company change-control procedures related to implementing security patches and software modifications, and verify that the procedures require items 6.4.1 – 6.4.4 below.			
	6.4.b For a sample of system components and recent changes/security patches, trace those changes back to related change control documentation. For each change examined, perform the following:			
6.4.1 Documentation of impact	6.4.1 Verify that documentation of customer impact is included in the change control documentation for each sampled change.			
6.4.2 Management sign-off by appropriate parties	6.4.2 Verify that management sign-off by appropriate parties is present for each sampled change.			
6.4.3 Testing of operational functionality	6.4.3 Verify that operational functionality testing is performed for each sampled change.			
6.4.4 Back-out procedures	6.4.4 Verify that back-out procedures are prepared for each sampled change			
6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the <i>Open Web Application Security Project Guide</i> . Cover prevention of common coding vulnerabilities in software development processes, to include the following: <i>Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.</i>	6.5.a Obtain and review software development processes for any web-based applications. Verify that processes require training in secure coding techniques for developers, and are based on guidance such as the OWASP guide (http://www.owasp.org).			
	6.5.b Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.			
	6.5.c Verify that processes are in place to ensure that web applications are not vulnerable to the following:			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.5.1 Cross-site scripting (XSS)	6.5.1 Cross-site scripting (XSS) (Validate all parameters before inclusion.)			
6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.	6.5.2 Injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries.)			
6.5.3 Malicious file execution	6.5.3 Malicious file execution (Validate input to verify application does not accept filenames or files from users.)			
6.5.4 Insecure direct object references	6.5.4 Insecure direct object references (Do not expose internal object references to users.)			
6.5.5 Cross-site request forgery (CSRF)	6.5.5 Cross-site request forgery (CSRF) (Do not reply on authorization credentials and tokens automatically submitted by browsers.)			
6.5.6 Information leakage and improper error handling	6.5.6 Information leakage and improper error handling (Do not leak information via error messages or other means.)			
6.5.7 Broken authentication and session management	6.5.7 Broken authentication and session management (Properly authenticate users and protect account credentials and session tokens.)			
6.5.8 Insecure cryptographic storage	6.5.8 Insecure cryptographic storage (Prevent cryptographic flaws.)			
6.5.9 Insecure communications	6.5.9 Insecure communications (Properly encrypt all authenticated and sensitive communications.)			
6.5.10 Failure to restrict URL access	6.5.10 Failure to restrict URL access (Consistently enforce access control in presentation layer and business logic for all URLs.)			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by <i>either</i> of the following methods: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ▪ Installing a web-application firewall in front of public-facing web applications	6.6 For <i>public-facing</i> web applications, ensure that <i>either</i> one of the following methods are in place as follows: ▪ Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows: – At least annually – After any changes – By an organization that specializes in application security – That all vulnerabilities are corrected – That the application is re-evaluated after the corrections ▪ Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks. <i>Note: “An organization that specializes in application security” can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.</i>			

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

“Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	7.1 Obtain and examine written policy for data control, and verify that the policy incorporates the following:			
7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	7.1.1 Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.			
7.1.2 Assignment of privileges is based on individual personnel's job classification and function	7.1.2 Confirm that privileges are assigned to individuals based on job classification and function (also called “role-based access control” or RBAC).			
7.1.3 Requirement for an authorization form signed by management that specifies required privileges	7.1.3 Confirm that an authorization form is required for all access, that it must specify required privileges, and that it must be signed by management.			
7.1.4 Implementation of an automated access control system	7.1.4 Confirm that access controls are implemented via an automated access control system.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	7.2 Examine system settings and vendor documentation to verify that an access control system is implemented as follows:			
7.2.1 Coverage of all system components	7.2.1 Confirm that access control systems are in place on all system components.			
7.2.2 Assignment of privileges to individuals based on job classification and function	7.2.2 Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.			
7.2.3 Default "deny-all" setting	7.2.3 Confirm that the access control systems has a default "deny-all" setting. <i>Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.</i>			

Requirement 8: Assign a unique ID to each person with computer access.

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	8.1 Verify that all users are assigned a unique ID for access to system components or cardholder data.			
8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: ▪ Password or passphrase ▪ Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)	8.2 To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following: ▪ Obtain and examine documentation describing the authentication method(s) used. ▪ For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).			
8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	8.3 To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that both a password and an additional authentication item (for example, smart card, token, PIN) are required.			
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in <i>PCI DSS Glossary of Terms, Abbreviations, and Acronyms</i>).	8.4.a For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage.			
	8.4.b For service providers only, observe password files to verify that customer passwords are encrypted.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/Comments
8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:	8.5 Review procedures and interview personnel to verify that procedures are implemented for user authentication and password management, by performing the following:			
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	8.5.1.a Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to company policy by performing the following: - Obtain and examine an authorization form for each ID. - Verify that the sampled user IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained), by tracing information from the authorization form to the system.			
8.5.2 Verify user identity before performing password resets.	8.5.2 Examine password procedures and observe security personnel to verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the password is reset.			
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use.	8.5.3 Examine password procedures and observe security personnel to verify that first-time passwords for new users are set to a unique value for each user and changed after first use.			
8.5.4 Immediately revoke access for any terminated users.	8.5.4 Select a sample of employees terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed.			
8.5.5 Remove/disable inactive user accounts at least every 90 days.	8.5.5 Verify that inactive accounts over 90 days old are either removed or disabled.			
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed.	8.5.6 Verify that any accounts used by vendors to support and maintain system components are disabled, enabled only when needed by the vendor, and monitored while being used.			
8.5.7 Communicate password procedures and policies to all users who have access to cardholder data.	8.5.7 Interview the users from a sample of user IDs, to verify that they are familiar with password procedures and policies.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.5.8 Do not use group, shared, or generic accounts and passwords.	8.5.8.a For a sample of system components, examine user ID lists to verify the following - Generic user IDs and accounts are disabled or removed. - Shared user IDs for system administration activities and other critical functions do not exist. - Shared and generic user IDs are not used to administer any system components.			
	8.5.8.b Examine password policies/procedures to verify that group and shared passwords are explicitly prohibited.			
	8.5.8.c Interview system administrators to verify that group and shared passwords are not distributed, even if requested.			
8.5.9 Change user passwords at least every 90 days.	8.5.9 For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days. For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to change periodically and that customers are given guidance as to when, and under what circumstances, passwords must change.			
8.5.10 Require a minimum password length of at least seven characters.	8.5.10 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long. For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to meet minimum length requirements.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.5.11 Use passwords containing both numeric and alphabetic characters.	8.5.11 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters. For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to contain both numeric and alphabetic characters.			
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	8.5.12 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords. For service providers only, review internal processes and customer/user documentation to verify that new customer passwords cannot be the same as the previous four passwords.			
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	8.5.13 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that a user's account is locked out after not more than six invalid logon attempts. For service providers only, review internal processes and customer/user documentation to verify that customer accounts are temporarily locked-out after not more than six invalid access attempts.			
8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	8.5.14 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.			
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.	8.5.15 For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/Comments
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.	8.5.16.a Review database and application configuration settings and verify that user authentication and access to databases includes the following: - All users are authenticated prior to access. - All user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures). - Direct access or queries to databases are restricted to database administrators.			
	8.5.16.b Review database applications and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).			

Requirement 9: Restrict physical access to cardholder data.

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	9.1 Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. - Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. - Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.			
9.1.1 Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. <i>Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.</i>	9.1.1 Verify that video cameras or other access control mechanisms are in place to monitor the entry/exit points to sensitive areas. Video cameras or other mechanisms should be protected from tampering or disabling. Verify that video cameras or other mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months.			
9.1.2 Restrict physical access to publicly accessible network jacks.	9.1.2 Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized employees. For example, conference rooms used to host visitors should not have network ports enabled with DHCP. Alternatively, verify that visitors are escorted at all times in areas with active network jacks.			
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.	9.1.3 Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. <i>For purposes of this requirement, "employee" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.</i>	9.2.a Review processes and procedures for assigning badges to employees, and visitors, and verify these processes include the following: - Granting new badges, changing access requirements, and revoking terminated employee and expired visitor badges - Limited access to badge system			
	9.2.b Observe people within the facility to verify that it is easy to distinguish between employees and visitors.			
9.3 Make sure all visitors are handled as follows:	9.3 Verify that employee/visitor controls are in place as follows:			
9.3.1 Authorized before entering areas where cardholder data is processed or maintained	9.3.1 Observe visitors to verify the use of visitor ID badges. Attempt to gain access to the data center to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data.			
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employee	9.3.2 Examine employee and visitor badges to verify that ID badges clearly distinguish employees from visitors/outside and that visitor badges expire.			
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration	9.3.3 Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration.			
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	9.4.a Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.			
	9.4.b Verify that the log contains the visitor's name, the firm represented, and the employee authorizing physical access, and is retained for at least three months.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.	9.5 Verify that the storage location is reviewed at least annually to determine that back-up media storage is secure.			
9.6 Physically secure all paper and electronic media that contain cardholder data.	9.6 Verify that procedures for protecting cardholder data include controls for physically securing paper and electronic media (including computers, removable electronic media, networking, and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes).			
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data, including the following:	9.7 Verify that a policy exists to control distribution of media containing cardholder data, and that the policy covers all distributed media including that distributed to individuals.			
9.7.1 Classify the media so it can be identified as confidential.	9.7.1 Verify that all media is classified so that it can be identified as "confidential."			
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.	9.7.2 Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery method that can be tracked.			
9.8 Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when media is distributed to individuals).	9.8 Select a recent sample of several days of offsite tracking logs for all media containing cardholder data, and verify the presence in the logs of tracking details and proper management authorization.			
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.	9.9 Obtain and examine the policy for controlling storage and maintenance of hardcopy and electronic media and verify that the policy requires periodic media inventories.			
9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	9.9.1 Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:	9.10 Obtain and examine the periodic media destruction policy and verify that it covers all media containing cardholder data and confirm the following:			
9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	9.10.1.a Verify that hard-copy materials are cross-cut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.			
	9.10.1.b Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a “to-be-shredded” container has a lock preventing access to its contents.			
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	9.10.2 Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).			

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	10.1 Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.			
10.2 Implement automated audit trails for all system components to reconstruct the following events:	10.2 Through interviews, examination of audit logs, and examination of audit log settings, perform the following:			
10.2.1 All individual accesses to cardholder data	10.2.1 Verify all individual access to cardholder data is logged.			
10.2.2 All actions taken by any individual with root or administrative privileges	10.2.2 Verify actions taken by any individual with root or administrative privileges is logged.			
10.2.3 Access to all audit trails	10.2.3 Verify access to all audit trails is logged.			
10.2.4 Invalid logical access attempts	10.2.4 Verify invalid logical access attempts are logged.			
10.2.5 Use of identification and authentication mechanisms	10.2.5 Verify use of identification and authentication mechanisms is logged.			
10.2.6 Initialization of the audit logs	10.2.6 Verify initialization of audit logs is logged.			
10.2.7 Creation and deletion of system-level objects	10.2.7 Verify creation and deletion of system level objects are logged.			
10.3 Record at least the following audit trail entries for all system components for each event:	10.3 Through interviews and observation, for each auditable event (from 10.2), perform the following:			
10.3.1 User identification	10.3.1 Verify user identification is included in log entries.			
10.3.2 Type of event	10.3.2 Verify type of event is included in log entries.			
10.3.3 Date and time	10.3.3 Verify date and time stamp is included in log entries.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.3.4 Success or failure indication	10.3.4 Verify success or failure indication is included in log entries.			
10.3.5 Origination of event	10.3.5 Verify origination of event is included in log entries.			
10.3.6 Identity or name of affected data, system component, or resource	10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.			
10.4 Synchronize all critical system clocks and times.	10.4 Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented:			
	10.4.a Verify that a known, stable version of NTP (Network Time Protocol) or similar technology, kept current per PCI DSS Requirements 6.1 and 6.2, is used for time synchronization.			
	10.4.b Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]			
	10.4.c Verify that specific external hosts are designated from which the timeservers will accept NTP time updates (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). See www.ntp.org for more information			
10.5 Secure audit trails so they cannot be altered.	10.5 Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.5.1 Limit viewing of audit trails to those with a job-related need.	10.5.1 Verify that only individuals who have a job-related need can view audit trail files.			
10.5.2 Protect audit trail files from unauthorized modifications.	10.5.2 Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.			
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	10.5.3 Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.			
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.	10.5.4 Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.			
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	10.5.5 Verify the use of file-integrity monitoring or change-detection software for logs by examining system settings and monitored files and results from monitoring activities.			
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). <i>Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6</i>	10.6.a Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.			
	10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components.			
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	10.7.a Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year.			
	10.7.b Verify that audit logs are available for at least one year and processes are in place to restore at least the last three months' logs for immediate analysis.			

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	11.1.a Verify that a wireless analyzer is used at least quarterly, or that a wireless IDS/IPS is implemented and configured to identify all wireless devices.			
	11.1.b If a wireless IDS/IPS is implemented, verify the configuration will generate alerts to personnel.			
	11.1 c Verify the organization's Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.			
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). <i>Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.</i>	11.2.a Inspect output from the most recent four quarters of internal network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder data environment occurs. Verify that the scan process includes rescans until passing results are obtained. <i>Note: External scans conducted after network changes, and internal scans, may be performed by the company's qualified internal personnel or third parties.</i>			
	11.2.b Verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security Scanning Procedures, by inspecting output from the four most recent quarters of external vulnerability scans to verify that: - Four quarterly scans occurred in the most recent 12-month period; - The results of each scan satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities); - The scans were completed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. <i>Note: It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the</i>			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
	<i>assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.</i>			
	11.2.c Verify that internal and/or external scanning is performed after any significant change in the network, by inspecting scan results for the last year. Verify that the scan process includes rescans until passing results are obtained.			
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:	11.3.a Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. Verify that noted vulnerabilities were corrected and testing repeated.			
	11.3.b Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).			
11.3.1 Network-layer penetration tests	11.3.1 Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems.			
11.3.2 Application-layer penetration tests	11.3.2 Verify that the penetration test includes application-layer penetration tests. For web applications, the tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.			
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.	11.4.a Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic in the cardholder data environment is monitored.			
	11.4.b Confirm IDS and/or IPS are configured to alert personnel of suspected compromises.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
	11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.			
11.5 Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. <i>Note: For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).</i>	11.5 Verify the use of file-integrity monitoring products within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: ▪ System executables ▪ Application executables ▪ Configuration and parameter files ▪ Centrally stored, historical or archived, log and audit files			

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, “employees” refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are “resident” on the company’s site.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/Comments
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	12.1 Examine the information security policy and verify that the policy is published and disseminated to all relevant system users (including vendors, contractors, and business partners).			
12.1.1 Addresses all PCI DSS requirements.	12.1.1 Verify that the policy addresses all PCI DSS requirements.			
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	12.1.2 Verify that the information security policy includes an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.			
12.1.3 Includes a review at least once a year and updates when the environment changes.	12.1.3 Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.			
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	12.2.a Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.3 Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	12.3 Obtain and examine the policy for critical employee-facing technologies and perform the following:			
12.3.1 Explicit management approval	12.3.1 Verify that the usage policies require explicit management approval to use the technologies.			
12.3.2 Authentication for use of the technology	12.3.2 Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (for example, token).			
12.3.3 A list of all such devices and personnel with access	12.3.3 Verify that the usage policies require a list of all devices and personnel authorized to use the devices.			
12.3.4 Labeling of devices with owner, contact information, and purpose	12.3.4 Verify that the usage policies require labeling of devices with owner, contact information, and purpose.			
12.3.5 Acceptable uses of the technology	12.3.5 Verify that the usage policies require acceptable uses for the technology.			
12.3.6 Acceptable network locations for the technologies	12.3.6 Verify that the usage policies require acceptable network locations for the technology.			
12.3.7 List of company-approved products	12.3.7 Verify that the usage policies require a list of company-approved products.			
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	12.3.8 Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.			
12.3.9 Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use	12.3.9 Verify that the usage policies require activation of remote-access technologies used by vendors only when needed by vendors, with immediate deactivation after use.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/Comments
12.3.10 When accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media.	12.3.10 Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives, and removable electronic media when accessing such data via remote-access technologies.			
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	12.4 Verify that information security policies clearly define information security responsibilities for both employees and contractors.			
12.5 Assign to an individual or team the following information security management responsibilities:	12.5 Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:			
12.5.1 Establish, document, and distribute security policies and procedures.	12.5.1 Verify that responsibility for creating and distributing security policies and procedures is formally assigned.			
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	12.5.2 Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.			
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	12.5.3 Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned.			
12.5.4 Administer user accounts, including additions, deletions, and modifications	12.5.4 Verify that responsibility for administering user account and authentication management is formally assigned.			
12.5.5 Monitor and control all access to data.	12.5.5 Verify that responsibility for monitoring and controlling all access to data is formally assigned.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/Comments
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.	12.6.a Verify the existence of a formal security awareness program for all employees.			
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:			
12.6.1 Educate employees upon hire and at least annually.	12.6.1.a Verify that the security awareness program provides multiple methods of communicating awareness and educating employees (for example, posters, letters, memos, web based training, meetings, and promotions).			
	12.6.1.b Verify that employees attend awareness training upon hire and at least annually.			
12.6.2 Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures.	12.6.2 Verify that the security awareness program requires employees to acknowledge (for example, in writing or electronically) at least annually that they have read and understand the company's information security policy.			
12.7 Screen potential employees (see definition of "employee" at 9.2 above) prior to hire to minimize the risk of attacks from internal sources. <i>For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.</i>	12.7 Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on employees prior to hire who will have access to cardholder data or the cardholder data environment. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)			
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	12.8 If the entity being assessed shares cardholder data with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), through observation, review of policies and procedures, and review of supporting documentation, perform the following:			
12.8.1 Maintain a list of service providers.	12.8.1 Verify that a list of service providers is maintained.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	12.8.2 Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data.			
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	12.8.3 Verify that policies and procedures are documented and were followed including proper due diligence prior to engaging any service provider.			
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status.	12.8.4 Verify that the entity assessed maintains a program to monitor its service providers' PCI DSS compliance status.			
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	12.9 Obtain and examine the Incident Response Plan and related procedures and perform the following:			

(12.9 continued on next page)

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: ▪ Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum ▪ Specific incident response procedures ▪ Business recovery and continuity procedures ▪ Data back-up processes ▪ Analysis of legal requirements for reporting compromises ▪ Coverage and responses of all critical system components ▪ Reference or inclusion of incident response procedures from the payment brands	12.9.1 Verify that the Incident Response Plan includes: ▪ Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum ▪ Specific incident response procedures, ▪ Business recovery and continuity procedures, ▪ Data back-up processes ▪ Analysis of legal requirements for reporting compromises (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database) ▪ Coverage and responses for all critical system components ▪ Reference or inclusion of incident response procedures from the payment brands			
12.9.2 Test the plan at least annually.	12.9.2 Verify that the plan is tested at least annually.			
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	12.9.3 Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.			
12.9.4 Provide appropriate training to staff with security breach response responsibilities.	12.9.4 Verify through observation and review of policies that staff with security breach responsibilities are periodically trained.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/Comments
12.9.5 Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.	12.9.5 Verify through observation and review of processes that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan.			
12.9.6 Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	12.9.6 Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.			

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

Requirement A.1: Shared hosting providers must protect the cardholder data environment

As referenced in Requirement 12.8, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. <i>Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.</i>	A.1 Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A.1.1 through A.1.4 below.			
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	A.1.1 If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: - No entity on the system can use a shared web server user ID. - All CGI scripts used by an entity must be created and run as the entity's unique user ID.			

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
A.1.2 Restrict each entity's access and privileges to own cardholder data environment only.	A.1.2.a Verify the user ID of any application process is not a privileged user (root/admin).			
	A.1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.). IMPORTANT: An entity's files may not be shared by group.			
	A.1.2.c Verify an entity's users do not have write access to shared system binaries.			
	A.1.2.d Verify that viewing of log entries is restricted to the owning entity.			
	A.1.2.e To ensure each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions, resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources: ▪ Disk space ▪ Bandwidth ▪ Memory ▪ CPU			
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	A.1.3.a Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: ▪ Logs are enabled for common third-party applications. ▪ Logs are active by default. ▪ Logs are available for review by the owning entity. ▪ Log locations are clearly communicated to the owning entity.			
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	A.1.4 Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.			

Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Navigating PCI DSS* for the intent of each PCI DSS requirement.)
3. Be “above and beyond” other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

When evaluating “above and beyond” for compensating controls, consider the following:

Note: The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.

- a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).
 - b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review. For example, two-factor authentication is a PCI DSS requirement for remote access. Two-factor authentication *from within the internal network* can also be considered as a compensating control for non-console administrative access when transmission of encrypted passwords cannot be supported. Two-factor authentication may be an acceptable compensating control if; (1) it meets the intent of the original requirement by addressing the risk of intercepting clear-text administrative passwords; and (2) it is set up properly and in a secure environment.
 - c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) two-factor authentication from within the internal network.
4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in the Report on Compliance in the corresponding PCI DSS requirement section.

Note: Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	

Compensating Controls Worksheet – Completed Example

Use this worksheet to define compensating controls for any requirement where “YES” was checked and compensating controls were mentioned in the “Special” column.

Requirement Number: 8.1—Are all users identified with a unique user name before allowing them to access system components or cardholder data?

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	<i>Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a “root” login. It is not possible for Company XYZ to manage the “root” login nor is it feasible to log all “root” activity by each user.</i>
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	<i>The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.</i>
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	<i>Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.</i>
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	<i>Company XYZ is going to require all users to log into the servers from their desktops using the SU command. SU allows a user to access the “root” account and perform actions under the “root” account but is able to be logged in the SU-log directory. In this way, each user’s actions can be tracked through the SU account.</i>
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	<i>Company XYZ demonstrates to assessor that the SU command being executed and that those individuals utilizing the command are logged to identify that the individual is performing actions under root privileges</i>
6. Maintenance	Define process and controls in place to maintain compensating controls.	<i>Company XYZ documents processes and procedures to ensure SU configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually tracked or logged</i>



Appendix D: Attestation of Compliance – Merchants
**Payment Card Industry (PCI)
Data Security Standard**

**Attestation of Compliance for
Onsite Assessments – Merchants**

Version 1.2

October 2008

Instructions for Submission

This document must be completed by a Qualified Security Assessor (QSA) or merchant (if merchant internal audit performs validation) as a declaration of the merchant's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and submit to the acquirer or requesting payment brand.

Part 1. Qualified Security Assessor Company Information

Company Name:					
Lead QSA Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP:	
URL:					

Part 2. Merchant Organization Information

Company Name:		DBA(s):			
Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP:	
URL:					

Part 2a. Type of Merchant Business (check all that apply)

- | | | |
|---|---|---|
| ☐ Retailer | ☐ Telecommunication | ☐ Grocery and Supermarkets |
| ☐ Petroleum | ☐ E-Commerce | ☐ Mail/Telephone-Order |
| ☐ Travel & Entertainment | ☐ Others (please specify): | |

List facilities and locations included in PCI DSS review:

Part 2b. Relationships

Does your company have a relationship with one or more third-party agents (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc)? ☐ Yes ☐ No

Does your company have a relationship with more than one acquirer? ☐ Yes ☐ No

Part 2c. Transaction Processing

Payment Application in use:

Payment Application Version:

Part 3. PCI DSS Validation

Based on the results noted in the Report on Compliance (“ROC”) dated *(date of ROC)*, *(QSA Name/Merchant Name)* asserts the following compliance status for the entity identified in Part 2 of this document as of *(date)* (check one):

- ☐ **Compliant:** All requirements in the ROC are marked “in place⁴,” and a passing scan has been completed by the PCI SSC Approved Scanning Vendor (*ASV Name*) thereby *(Merchant Company Name)* has demonstrated full compliance with the PCI DSS *(insert version number)*.
- ☐ **Non-Compliant:** Some requirements in the ROC are marked “not in place,” resulting in an overall **NON-COMPLIANT** rating, **or** a passing scan has not been completed by a PCI SSC Approved Scanning Vendor, thereby *(Merchant Company Name)* has not demonstrated full compliance with the PCI DSS.
- Target Date** for Compliance:
- An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

QSA/Merchant confirms:

- ☐ The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *(insert version number)*, and was completed according to the instructions therein.
- ☐ All information within the above-referenced ROC and in this attestation fairly represents the results of the assessment in all material respects.
- ☐ The merchant has confirmed with the payment application vendor that their payment application does not store sensitive authentication data after authorization.
- ☐ The merchant has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times.
- ☐ No evidence of magnetic stripe (i.e., track) data⁵, CAV2, CVC2, CID, or CVV2 data⁶, or PIN data⁷ storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. QSA and Merchant Acknowledgments

Signature of Lead QSA ↑		Date:
Lead QSA Name:		Title:
Signature of Merchant Executive Officer ↑		Date:
Merchant Executive Officer Name:		Title:

⁴ “In place” results should include compensating controls reviewed by the QSA/merchant Internal Audit. If compensating controls are determined to sufficiently mitigate the risk associated with the requirement, the QSA should mark the requirement as “in place”.

⁵ Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

⁶ The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.

⁷ Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate “Compliance Status” for each requirement. If you answer “No” to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with your acquirer or the payment brand(s) before completing Part 4 since not all payment brands require this section.*

PCI Requirement	Description	Compliance Status (Select One)	Remediation Date and Actions (if Compliance Status is “No”)
1	Install and maintain a firewall configuration to protect cardholder data.	☐ Yes ☐ No	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	☐ Yes ☐ No	
3	Protect stored cardholder data.	☐ Yes ☐ No	
4	Encrypt transmission of cardholder data across open, public networks.	☐ Yes ☐ No	
5	Use and regularly update anti-virus software.	☐ Yes ☐ No	
6	Develop and maintain secure systems and applications.	☐ Yes ☐ No	
7	Restrict access to cardholder data by business need to know.	☐ Yes ☐ No	
8	Assign a unique ID to each person with computer access.	☐ Yes ☐ No	
9	Restrict physical access to cardholder data.	☐ Yes ☐ No	
10	Track and monitor all access to network resources and cardholder data.	☐ Yes ☐ No	
11	Regularly test security systems and processes.	☐ Yes ☐ No	
12	Maintain a policy that addresses information security.	☐ Yes ☐ No	





Appendix E: Attestation of Compliance – Service Providers
**Payment Card Industry (PCI)
Data Security Standard**

**Attestation of Compliance for
Onsite Assessments – Service Providers**

Version 1.2

October 2008

Instructions for Submission

The Qualified Security Assessor (QSA) and Service Provider must complete this document as a declaration of the Service Provider's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and submit to the requesting payment brand.

Part 1. Qualified Security Assessor Company Information

Company Name:					
Lead QSA Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP:	
URL:					

Part 2. Service Provider Organization Information

Company Name:		DBA(s):			
Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP:	
URL:					

Part 2a. Services Provided (check all that apply)

☐ Authorization	☐ Loyalty Programs	☐ 3-D Secure Access Control Server
☐ Switching	☐ IPSP (E-commerce)	☐ Process Magnetic-Stripe Transactions
☐ Payment Gateway	☐ Clearing & Settlement	☐ Process MO/TO Transactions
☐ Hosting	☐ Issuing Processing	☐ Others (please specify):

List facilities and locations included in PCI DSS review:

Part 2b. Relationships

Does your company have a relationship with one or more third-party service providers (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc)? ☐ Yes ☐ No

Part 2c. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data?

Payment Application in use:

Payment Application Version:

Part 3. PCI DSS Validation

Based on the results noted in the Report on Compliance (“ROC”) dated *(date of ROC)*, *(QSA Name)* asserts the following compliance status for the entity identified in Part 2 of this document as of *(date)* (check one):

- ☐ **Compliant:** All requirements in the ROC are marked “in place⁸,” and a passing scan has been completed by the PCI SSC Approved Scanning Vendor (*ASV Name*) thereby (*Service Provider Name*) has demonstrated full compliance with the PCI DSS (*insert version number*).
- ☐ **Non-Compliant:** Some requirements in the ROC are marked “not in place,” resulting in an overall **NON-COMPLIANT** rating, **or** a passing scan has not been completed by a PCI SSC Approved Scanning Vendor, thereby (*Service Provider Name*) has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

QSA and Service Provider confirm:

- ☐ The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version (*insert version number*), and was completed according to the instructions therein.
- ☐ All information within the above-referenced ROC and in this attestation fairly represents the results of the assessment in all material respects.
- ☐ The Service Provider has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times.
- ☐ No evidence of magnetic stripe (i.e., track) data⁹, CAV2, CVC2, CID, or CVV2 data¹⁰, or PIN data¹¹ storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. QSA and Service Provider Acknowledgments

<i>Signature of Lead QSA</i> ↑		<i>Date:</i>
<i>Lead QSA Name:</i>	<i>Title:</i>	
<i>Signature of Service Provider Executive Officer</i> ↑		<i>Date:</i>
<i>Service Provider Executive Officer Name:</i>	<i>Title:</i>	

⁸ “In place” results should include compensating controls reviewed by the QSA. If compensating controls are determined to sufficiently mitigate the risk associated with the requirement, the QSA should mark the requirement as “in place”.

⁹ Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

¹⁰ The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.

¹¹ Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

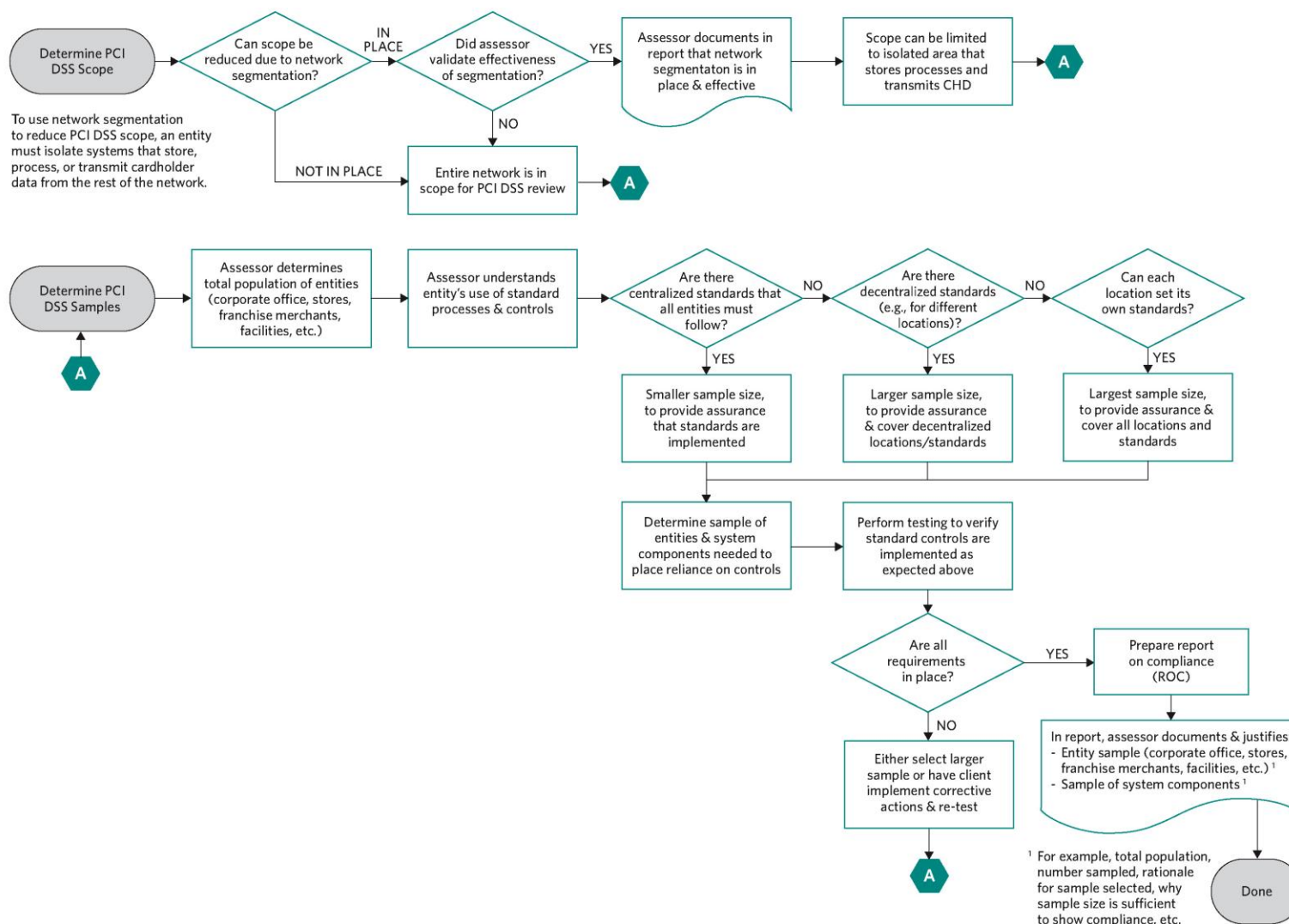
Part 4. Action Plan for Non-Compliant Status

Please select the appropriate “Compliance Status” for each requirement. If you answer “No” to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with the payment brand(s) before completing Part 4 since not all payment brands require this section.*

PCI Requirement	Description	Compliance Status (Select One)	Remediation Date and Actions (if Compliance Status is “No”)
1	Install and maintain a firewall configuration to protect cardholder data.	☐ Yes ☐ No	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	☐ Yes ☐ No	
3	Protect stored cardholder data.	☐ Yes ☐ No	
4	Encrypt transmission of cardholder data across open, public networks.	☐ Yes ☐ No	
5	Use and regularly update anti-virus software.	☐ Yes ☐ No	
6	Develop and maintain secure systems and applications.	☐ Yes ☐ No	
7	Restrict access to cardholder data by business need to know.	☐ Yes ☐ No	
8	Assign a unique ID to each person with computer access.	☐ Yes ☐ No	
9	Restrict physical access to cardholder data.	☐ Yes ☐ No	
10	Track and monitor all access to network resources and cardholder data.	☐ Yes ☐ No	
11	Regularly test security systems and processes.	☐ Yes ☐ No	
12	Maintain a policy that addresses information security.	☐ Yes ☐ No	



Appendix F: PCI DSS Reviews — Scoping and Selecting Samples





What To Do If Compromised

Visa Fraud Control and Investigations Procedures

December 2008
Version 1.0 (U.S.)



Table of Contents

Introduction	3
Identifying and Detecting Security Breaches.....	4
Attack Vectors	5
Steps and Requirements for Compromised Entities.....	9
Steps and Requirements for Visa Clients (Acquirers and Issuers)	12
Requirements for Account Data Requests	15
Compromised Account Management System (CAMS).....	17
Appendix A: Initial Investigation Request.....	19
Appendix B: Forensic Investigation Guideline	23
Appendix C: Preliminary Incident Report Template	28
Appendix D: Final Incident Report Template.....	29
Appendix E: Account Data Layout Format	35
Appendix F: PIN Security Requirements	46
Appendix G: List of Supporting Documents.....	51
Appendix H: Glossary of Terms	52
Appendix I: Investigation Definitions.....	58
Appendix J: Secret Service Electronic Crimes Task Force (ECTF).....	59
Appendix K: Federal Bureau of Investigations (FBI)	60

Introduction

What constitutes a security incident? The answer to this question is crucial to any organization looking to minimize the impact an incident might have on its business operations.

In general, incidents may be defined as deliberate electronic attacks on communications or information processing systems. Whether initiated by a disgruntled employee, a malicious competitor, or a misguided hacker, deliberate attacks often cause damage and disruption to the payment system. How you respond to and handle an attack on your company's information systems will determine how well you will be able to control the costs and consequences that could result. For these reasons, the extent to which you prepare for security incidents, and work with Visa Inc., will be vitally important to the protection of your company's key information.

In the event of a security incident, Visa clients and their agents must take immediate action to investigate the incident, limit the exposure of cardholder data, notify Visa, and report investigation findings to Visa.¹

The *What To Do If Compromised* guide is intended for Visa clients (i.e., acquirers and issuers), merchants, agents, and third-party service providers. It contains step-by-step instructions on how to respond to a security incident and provides specific time frames for the delivery of information or reports outlining actions taken by Visa, its clients, and its agents.

In addition to the general instructions provided here, Visa may also require an investigation that includes, but is not limited to, access to premises and all pertinent records including copies of analysis.

¹ Visa U.S.A. Inc. *Operating Regulations*—Section 2.3.F.3, Loss or Theft of Account or Transaction Information; Section 2.3.F.4, Investigations; and Section 2.3, General Security Requirements. Visa U.S.A. Plus System, Inc. *Bylaws and Operating Regulations*—Section 1.19, Customer Information Security Program; Visa U.S.A. Interlink Network, Inc. *Bylaws and Operating Regulations*—Section 2.4, Investigation of Merchants; Section 2.6, Cardholder Information Security Program; Section 2.8, Loss or Theft of Account Information. Visa U.S.A. Inc. *Operating Regulations* are available at www.visa.com.

Identifying and Detecting Security Breaches

It is often difficult to detect when a system has been attacked or an intrusion has taken place. Distinguishing normal events from those that are related to an attack or intrusion is a critical part of maintaining a secure payment processing environment.

Security breaches come in many different forms and, while detecting them may be challenging, there are certain signs that tend to appear when a security breach has occurred:

- Unknown or unexpected outgoing Internet network traffic from the payment card environment
- Presence of unexpected IP addresses on store and wireless networks
- Unknown or unexpected network traffic from store to headquarter locations
- Unknown or unexpected services and applications configured to launch automatically on system boot
- Unknown files, software and devices installed on systems
- Anti-virus programs malfunctioning or becoming disabled for unknown reasons
- Failed login attempts in system authentication and event logs
- Vendor or third-party connections made to the cardholder environment without prior consent and/or a trouble ticket
- SQL Injection attempts in web server event logs
- Authentication event log modifications (i.e., unexplained event logs are being deleted)
- Suspicious after-hours file system activity (i.e., user login or after-hours activity to Point-of-Sale ("POS") server)
- Presence of .zip, .rar, .tar, and other types of unidentified compressed files containing cardholder data
- Presence of a rootkit, which hides certain files and processes in, for example, Explorer, the Task Manager, and other tools or commands
- Systems rebooting or shutting down for unknown reasons
- If you are running Microsoft, check Windows registry settings for hidden malicious code. (**Note:** Make sure you back up your registry keys before making any changes and consult with Microsoft Help and Support).

Attack Vectors

The following are examples of attack vectors that hackers use to gain unauthorized access to organization's systems and steal sensitive information, such as payment card data and passwords.

SQL Injection Attacks

SQL injection is a technique used to exploit Web-based applications that use client-supplied data in SQL queries. SQL injection attacks can occur as a result of unpatched Web servers, improperly designed applications (i.e, incorrectly filtered escape characters or error-type handling) or poorly configured Web and database servers.

The SQL attack methods most recently detected were targeted against Websites and Web applications that were improperly designed or resided on unpatched systems, making them susceptible to attack. These latest SQL injection attacks pose serious additional risks to cardholder data stored or transmitted within systems (e.g., Microsoft and UNIX-based) and networks connected to the affected environment.

Improperly Segmented Network Environment

Payment card account information has been compromised at organizations that lack proper network segmentation. This attack method originates on the Internet, resulting in penetration to the organization's payment card environment and often leading to costly remediation efforts and increased fraud attacks. Such compromises can often be prevented if the organization's networks are properly segmented, limiting intruders to non-sensitive parts of the network that do not contain payment card information.

Network segmentation is a concept that refers to the practice of splitting a network into functional segments and implementing an access control mechanism between each of the boundaries. The most common example of network segmentation is the separation between the Internet and an internal network using a firewall/router.

Malicious Code Attacks

Malicious codes or malware can be programs such as viruses, worms, Trojan applications, and scripts used by intruders to gain privileged access and capture passwords or other confidential information (e.g., user account information). Malicious code attacks are usually difficult to detect because certain viruses can be designed to modify their own signatures after inflicting a system and before spreading to another. Some malicious codes can also modify audit logs to hide unauthorized activities.

In recent investigations, Visa has identified malicious codes designed to capture payment card data. These are examples of malicious code attacks:

- **Malware that allows interactive command shell or backdoor.** This type of malware allows an intruder to run commands to the compromised system. In some cases, the malware is hard-coded with the intruder's Internet Protocol ("IP") address.

- **Packet sniffers.** Packet sniffing is the practice of using computer software or hardware to intercept and log traffic passing over a computer network. A packet sniffer, also known as a network analyzer or protocol analyzer, captures and interprets a stream or block of data (referred to as a "packet") traveling over a network.

Packet sniffers are typically used in conjunction with malicious software or malware. Once intruders gain entry into a critical system using backdoor programs or deploying rootkits, the sniffer programs are installed, making the malware more difficult to detect. Intruders can then "sniff" packets between network users and collect sensitive information such as usernames, passwords, payment card data or Social Security numbers. Once a critical system or network is compromised, sniffers are used to eavesdrop or spy on network users and activity. This combination of tools makes this attack scheme effective in compromising systems and networks.

- **Key logger malware.** Key logging is a method of capturing and recording keystrokes. There are key logger applications that are commercially available and are used by organizations to troubleshoot problems within computer systems. Visa Investigations reveal that there are key logger applications that are developed by intruders to capture payment card data and/or users credentials, such as passwords. The key logger captures information in real time and sends it directly to the intruder over the Internet. Additionally, newer advances provide the ability to intermittently capture screenshots from the key logged computer.

Key logger malware are widely available via the Internet and can be installed on virtually any operating system. Key loggers, like most malware, are distributed as part of a Trojan horse or virus, sent via e-mail (as an attachment or by clicking to an infected web link or site) or, in the worst case, installed by a hacker with direct access to a victim's computer.

Insecure Remote Access

Many Point-of Sale (“POS”) vendors, resellers and integrators have introduced remote access management products into the environments of organizations that they support. A variety of remote access solutions exists, ranging from command-line based (e.g., SSH, Telnet) to visually-driven packages (e.g., pcAnywhere, Virtual Network Computing, Remote Desktop). The use of remote management products comes with an inherent level of risk that may create a virtual backdoor on your system. The exploitation of improperly configured and unpatched remote management software tools is the method of attack most frequently used by hackers against POS payment systems. An improperly configured system can be vulnerable in the following ways:

- Failure to regularly update or patch a system can render the system vulnerable to exploits that defeat the security mechanisms built into the product.
- Lack of encryption or weak encryption algorithms can lead to the disclosure of access credentials.
- Use of default passwords can provide easy access to unauthorized individuals.
- Disabled logging mechanisms eliminate insight into system access activity and signs of intrusion.

Insecure Wireless

The adoption of wireless technology is on the rise among participants in the payment industry; particularly merchant retailers, many of whom use wireless technology for inventory systems or check-out efficiency (e.g., “line busting,” ringing up customers while they are in line). Wireless technologies have unique vulnerabilities; organizations must carefully evaluate the need for such technology and understand the risks, as well as the security requirements, before deploying wireless systems.

Following are some of the common methods used to attack wireless networks. These methods are widely documented on the Internet, complete with downloadable software and instructions.

- **Eavesdropping** — An attacker can gain access to a wireless network just by “listening” to traffic. Radio transmissions can be freely and easily intercepted by nearby devices or laptops. The sender or intended receiver has no means of knowing whether the transmission has been intercepted.

- **Rogue Access** — If a wireless Local Area Network (LAN) is part of an enterprise network, a compromise of the LAN may lead to the compromise of the enterprise network. An attacker with a rogue access point can fool a mobile station into authenticating with the rogue access point, thereby gaining access to the mobile station. This is known as a “trust problem,” and the only protection against it is an efficient access-authentication mechanism.
- **Denial of Service (DOS)** — Due to the nature of radio transmission, wireless LANs are vulnerable to denial-of-service attacks and radio interference. Such attacks can be used to disrupt business operations or to gather additional information for use in initiating another type of attack.
- **Man-in-the-Middle (MITM)** — Packet spoofing and impersonation, whereby traffic is intercepted midstream then redirected by an unauthorized individual for malicious purposes, are also valid threats.

For more information on additional attack vectors and mitigation strategies, please visit www.visa.com/cisp, under “Alerts, Bulletins and Webinars”.

Steps and Requirements for Compromised Entities

Entities that have experienced a suspected or confirmed security breach must take prompt action to help prevent additional exposure of cardholder data and ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS), PCI Payment Application Data Security Standard (PA-DSS)², and PCI PIN Security Requirements³.

1. Immediately contain and limit the exposure. Minimize data loss. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. Compromised entities should consult with their internal incident response team. To preserve evidence and facilitate the investigation:
 - Do not access or alter compromised system(s) (i.e., don't log on at all to the compromised system(s) and change passwords; do not log in as ROOT).
 - Do not turn the compromised system(s) off. Instead, isolate compromised systems(s) from the network (i.e., unplug network cable).
 - Preserve logs (i.e., security events, web, database, firewall, etc.)
 - Log all actions taken.
 - If using a wireless network, change the Service Set Identifier (SSID) on the wireless access point (WAP) and other systems that may be using this connection (with the exception of any systems believed to be compromised).
 - Be on "high" alert and monitor traffic on all systems with cardholder data.

² *Visa U.S.A. Inc. Operating Regulations*—Section 2.1.E.3, Loss or Theft of Account or Transaction Information; Section 2.1.E.4, Investigations; and Section 2.3, General Security Requirements. *Visa U.S.A. Plus System, Inc. Operating Regulations*—Section 1.19, Customer Information Security Program. *Visa U.S.A. Interlink Network, Inc. Operating Regulations*—Section 2.4, Investigation of Merchants; Section 2.6, Cardholder Information Security Program; Section 2.8, Loss or Theft of Account Information. Visa Operating Regulations are available at www.visa.com.

³ By submitting a Transaction through Interchange, an Acquirer warrants that required safeguards, as specified in the *PIN Management Requirements* documents, are protecting the Issuer's PIN. The Acquirer agrees to indemnify and hold harmless the Issuer for all Claims and Liabilities resulting from the Acquirer's breach of this warranty. *Visa U.S.A. Operating Regulations*—Section 1.16.B.45. *Visa U.S.A. Interlink Network, Inc. Bylaws and Operating Regulations*—Section 1.10.D.1. *Visa U.S.A. Plus System, Inc. Bylaws and Operating Regulations*—Section 1.10.C.

2. Alert all necessary parties immediately:
 - Your internal incident response team and information security group.
 - If you are a merchant, contact your merchant bank.
 - If you do not know the name and/or contact information for your merchant bank, notify Visa Incident Response Manager immediately:
 - U.S. – (650) 432-2978 or usfraudcontrol@visa.com
 - Canada – (416) 860-3090 or CanadaInvestigations@visa.com
 - Latin America & Caribbean – (305) 328-1713 or lacrmac@visa.com
 - Asia Pacific – (65) 96307672 or APIInvestigations@visa.com
 - CEMEA – +44 (0) 207-225-8600 or CEMEAFraudControl@visa.com

If you are a financial institution, contact the appropriate Visa region at the number provided above.
3. Notify the appropriate law enforcement agency. (See *Appendix J*, on page 59, for United States Secret Service Electronic Crimes Task Force contact information in your area.)

KEY POINT TO REMEMBER

To minimize the impact of a cardholder information security breach, Visa has created an Incident Response Team to assist in forensic investigations. In the event of a compromise, Visa will coordinate a team of forensic specialists to go onsite immediately to help identify security deficiencies and control exposure. The forensic information collected by this team is often used as evidence to prosecute criminals.

4. The compromised entity should consult with its legal department to determine if state notification laws are applicable.
5. Provide all compromised Visa, Interlink, and Plus accounts to the Visa acquiring bank or to Visa within ten (10) business days. All potentially compromised accounts must be provided and transmitted as instructed by the Visa acquiring bank and Visa. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. **Note:** If you are an issuer, provide foreign accounts or accounts from other financial institutions to Visa.

6. Within three (3) business days of the reported compromise, provide an Incident Report to the Visa client or to Visa. (See *Appendix C*, on page 28, for the Incident Report template.) If you are a financial institution, provide the Incident Report to Visa.

Note: If Visa deems necessary, an independent forensic investigation by a Visa-approved Qualified Incident Response Assessor (QIRA) will be initiated on the compromised entity. This policy applies to compromised financial institutions.

Steps and Requirements for Visa Clients (Acquirers and Issuers)

Notification	1. Immediately report to Visa the suspected or confirmed loss or theft of Visa cardholder data. Clients must contact the Visa Risk Management group immediately at the appropriate Visa region. 2. Within 48 hours, advise Visa whether the entity was in compliance with PCI DSS and, if applicable, PCI PA-DSS and PCI PIN Security requirements at the time of the incident. If so, provide appropriate proof.
Preliminary Investigation	3. Perform an initial investigation and provide written documentation to Visa within three (3) business days. The information provided will help Visa understand the potential exposure and assist entities in containing the incident. Documentation must include the steps taken to contain the incident.

FOR MORE INFORMATION

To find out more about conducting an initial investigation, see *Appendix A: Initial Investigation Request* on page 19.

Independent Forensic Investigation	If Visa deems necessary, an independent forensic investigation must be conducted by a QIRA. 4. Upon receipt of an initial independent forensic investigation notification from Visa, clients must: ▪ Identify the QIRA within five (5) business days. ▪ Ensure that the QIRA is engaged (or the contract is signed) within ten (10) business days. ▪ The QIRA must be onsite to conduct a forensic investigation within five (5) business days from the date the contract agreement is signed. The Visa client or compromised entity should engage the QIRA directly. However, Visa, has the right to engage a QIRA to perform a forensic investigation as it deems appropriate, and will assess all investigative costs to the client in addition to any fine that may be applicable.
------------------------------------	---

KEY POINT TO REMEMBER

The entity must have the QIRA evaluate whether the entity complies with each of the 32 PCI PIN Security Requirements, available on www.visa.com/pinsecurity

- | | |
|-----------------------------|--|
| | 5. If there is a suspected PIN compromise, the QIRA will perform a PIN security and key management investigation and a PCI PIN security assessment. |
| | 6. Provide a preliminary forensic report to Visa within five (5) business days from the onsite review. <i>The QIRA or the compromised entity can work with the appropriate region in the event that the preliminary report is delayed.</i> |
| | 7. Provide a final forensic report to Visa within ten (10) business days from the completion of the review. |
| PIN Security | 8. If there is a suspected PIN compromise, provide a PIN security report within ten (10) business days from the onsite review. This report should also review PIN-related cryptographic keys to determine if the keys might have been compromised. |
| Account Numbers | 9. Provide “at risk” account numbers to Visa within ten (10) business days from the date that Visa requests the account numbers. |
| Containment/
Remediation | 10. Ensure that the compromised entity has contained the incident and has implemented security recommendations provided by the QIRA, including any non-compliance with the PCI PIN Security Requirements. |
| | 11. If the entity is retaining full-track data, CVV2, and/or PIN blocks, ensure that the entity has removed the data (this includes any historical data). |
| | 12. Validate that full-track data, CVV2, and/or PIN blocks are no longer being stored on any systems. Even though this is the client’s responsibility, Visa requires that the validation be performed by the QIRA. |
| | 13. Submit a remediation plan to Visa within five (5) business days after receiving the final forensic report. As required by Visa, clients must provide a remediation plan with implementation dates related to findings identified by the QIRA.

A revised remediation plan must be provided to Visa, as needed. |
| | 14. Monitor and confirm that the compromised entity has implemented the action plan. |

**PCI DSS
Compliance**

15. Ensure that the compromised entity achieves full PCI compliance by adhering to the PCI DSS, PCI PA-DSS and, if applicable, the PCI PIN Security Requirements. Compliance validation is required per *Visa International Operating Regulations*.

KEY POINT TO REMEMBER

Please visit www.pcisecuritystandards.org for more information on PCI DSS and the PCI PIN Entry Device Testing Program. For more information on PCI PIN Security Requirements, please visit www.visa.com/pinsecurity.

Requirements for Account Data Requests

In the event of a compromise, Visa requires that “at risk” accounts be provided to Visa through Visa’s Compromised Account Management System (CAMS).

In some cases, Visa may require the entity to provide accounts via a CD using encryption software such as PGP⁴ or Winzip⁵ with 256-AES encryption and strong password. The following guidelines must be followed when providing accounts to Visa:

Account Data Format

- The account data provided must be **authorization** data only.
- File submitted must be a plain-text, comma delimited file containing account numbers and expiration dates. For example:
 - The card number, followed by a comma, followed by the expiration date in YYMM format:

4xxxxxxxxxxx1234,0801

KEY POINT TO REMEMBER

Visa may require additional data for further fraud analysis and will inform the compromised entity and the Visa client if additional data is required.

Please refer to *Appendix E* for information on the Advanced Account Data Format and Account Data File Layout.

1. Submitted data should be limited to **one** file. In cases where one file isn’t possible, make every effort to minimize total file counts. If multiple files are provided, all of them **MUST** be consistent (i.e., they **MUST** contain the same formatting and transaction details).
2. The following information must be provided in separate files and clearly labeled:
 - Signature and PIN-based transactions (Interlink and Plus)
 - Track and non-track data
 - Data sniffed/captured by the hacker
 - Data stored by the compromised entity
 - Data transferred out of the compromised entity’s network

⁴ PGP (Pretty Good Privacy) is a computer program that provides cryptographic privacy and authentication. For more information on PGP, go to www.pgp.com.

⁵ WinZip is a data compression utility with the ability to compress using 256-AES encryption. For more information on WinZip, go to www.winzip.com.

Account Data Upload

When providing a file to Visa via CAMS or copying to a CD, the user must provide a description of the data being uploaded or copied. For example:

1. Transaction date(s) of “at risk” accounts
2. Data elements at risk:
 - Primary Account Number (PAN)
 - Expiration date
 - Track 1 or 2
 - CVV2
 - PIN blocks
 - Other cardholder information, such as billing address, e-mail addresses, SSN, DOB, etc.
3. Name of compromised entity
4. Name of Visa investigator handling the incident

KEY POINT TO REMEMBER

Visa accounts copied to a CD or other removable media must be encrypted using PGP or Winzip with 256-AES encryption with strong password.

Compromised Account Management System (CAMS)

The Compromised Account Management System (CAMS) offers a secure and efficient way for acquirers, merchants, law enforcement agencies, and financial institutions to transmit compromised and recovered account data to and from Visa through an encrypted site. Using CAMS, acquirers, merchants, and law enforcement officers can upload potentially compromised and recovered accounts directly to Visa.

Subscribing financial institutions can access CAMS by logging on to www.us.visaonline.com and receive compromise alerts via e-mail regarding their accounts.

To Upload File(s):

1. Access the "Submit CAMS Alert" screen to upload your file data. At this screen, you must enter a description, indicate whether you are providing an expiration date, and select a file to upload from your hard drive.

Submit CAMS Alert

The screenshot shows the 'Submit CAMS Alert' form with the following elements and numbered steps:

- Step 2:** Points to the 'Select Visa Contact:' label and the '<select one>' dropdown menu.
- Step 3:** Points to the 'Enter a Brief Description: (255 characters max)' text area.
- Step 4:** Points to the 'Check if the file includes:' label and the 'Expiration Date' checkbox.
- Step 5:** Points to the 'Choose a file to upload:' label, the file input field, and the 'Browse...' button.
- Step 6:** Points to the 'Upload' button.
- Step 7:** Points to the 'Cancel' button.

There is also a 'Learn More' link with an information icon located above the 'Browse...' button.

2. From the drop down menu, select your assigned Visa contact. **This field is required.**
3. Enter a brief description of the files you are uploading for the compromise.
4. If applicable, indicate whether the file includes an expiration date. (Indicating an account expiration date will help the issuer identify which accounts are good candidates for monitoring.)

5. Click "Browse" to select a file from your local hard drive.
 - Files must be either plain text or a .zip file containing plain text files.
 - Files cannot exceed 100 MB in size.
 - The uploaded file should contain 11-19 digit account numbers.
6. Click the "Upload" button to begin the file transfer process. *The progress box will display how much of the upload has been completed.*
7. To stop the file transfer, click the "**Cancel**" button at any time.

To Upload Additional File(s):

After a successful upload, the "Submit CAMS Alert" screen will reappear with a message that confirms that your upload has been completed successfully. You will also be asked if you would like to add another file to the same alert. If you add another file, please remember that you will only be allowed to submit one description for each alert; the first description that you submit will apply.

If an error occurs during the upload, an error message will appear and you will be asked to upload the file again. You should also receive an e-mail message describing the upload error.

In response, you can either resubmit the file or contact the CAMS Administrator at VisaRiskManager@visa.com or 1-800-439-9013 for assistance.

Appendix A: Initial Investigation Request

Upon notification of a suspected account data compromise, Visa will request that the Visa client initiate a preliminary investigation of any entity involved in a potential track data, CVV2, and/or PIN compromise. The initial investigation will assist Visa in understanding the compromised entity's network environment.

To comply with Visa's initial investigation request, the Visa client must provide the following information:

KEY POINT TO REMEMBER

The information required below is applicable to suspected/confirmed compromised entities such as Visa clients, merchants, processors, or third-party service providers.

Entity Information

DESCRIPTION	RESPONSE
Name of entity	
Is entity a direct-connect to Visa?	
If entity is a merchant, provide the Merchant Category Code (MCC)	
Acquirer BIN	
Entity PCI DSS Level (e.g., Level 1-4)	
Entity PCI DSS Compliance Status (If compliant, please provide proof of PCI DSS compliance documentation.)	
If merchant, date entity began processing with acquirer	
If merchant, date entity stopped processing with acquirer (if applicable)	
Approximate number of transactions/accounts handled per year	
1) ATM	
2) POS PIN/Debit	
3) Credit	
If merchant, is entity corporate-owned or an individual franchise?	
If merchant, does entity have other locations? If so, please provide a list of locations, the name of the payment application, and version information.	

Network/Host Information

DESCRIPTION	RESPONSE
Is there Internet connectivity?	
Is there wireless connectivity?	
Does entity utilize a high-speed connection (e.g., cable modem, DSL)	
Is there remote access connectivity? If so, who has remote access?	
Is remote access always on or is it enabled upon request?	
What type of remote access software is used?	
Is the terminal PC-based or is it connected to a PC-based environment?	
Has entity noticed any abnormal activity on its systems?	
Is the entity retaining full track data, CVV2 or encrypted PIN blocks?	
How long is the data stored on the system(s)?	
Have there been any recent changes to the network and host such as: ▪ Upgrade to the payment application ▪ Installation of a firewall ▪ Installation of anti-virus program ▪ Changes to remote access connectivity	
Provide a transaction flow for credit and debit, as well as remote access to the network. The data flow must include: ▪ Cardholder data sent to a central corporate server or data center ▪ Upstream connection to third-party service providers ▪ Connection to entity bank/acquirer ▪ Remote access connection by third-party service providers or internal staff	

Third-Party Connectivity

DESCRIPTION	RESPONSE
Does the entity send transactions to a processor(s)? If so, who is the processor(s)?	
Name of payment application vendor	
Name of reseller, if applicable	
Is the entity hosted? If so, who is the hosting provider?	

List of Payment Applications and PIN Entry Device (PED) in Use

DESCRIPTION	RESPONSE
Payment application and version information	
Is this a corporate-mandated payment application and version?	
PIN Entry Device (PED) information, if applicable. Include the name of the PED firmware version. Visit www.pcisecuritystandards.org/pin for a list of PCI-approved PIN entry devices.	
Shopping cart and version information	
Are the payment applications in use PCI PA-DSS compliant? Visit www.visa.com/PABP for a list of PA-DSS compliant payment applications.	
Is entity using a compliant PED? Visit www.pcisecuritystandards.org/pin for a list of compliant PEDs.	

Potential Skimming/PED Tampering

DESCRIPTION	RESPONSE
Can entity trace legitimate transactions to a single employee, device, or lane(s)?	
Did entity have any employees who were employed for a short period of time?	
Did other employees notice suspicious behavior of the new employee (e.g., eager to handle all credit card transactions)?	
Is there any video surveillance and has it been reviewed?	
Can all PEDs be accounted for at all times?	
Are any of the POS PEDs in use listed on the November 2007 Security Alert available at www.visa.com/cisp ?	

Other Information

DESCRIPTION	RESPONSE
Has entity received complaints regarding fraudulent transactions from their customers?	
Has entity been contacted by law enforcement regarding fraudulent transactions?	
Can law enforcement provide intelligence that skimming groups are active in the area?	

Appendix B: Forensic Investigation Guideline

A Visa client or compromised entity must ensure that only a Visa-approved Qualified Incident Response Assessor (QIRA) is engaged to perform a forensic investigation. All QIRAs are required to adhere to the following forensic investigation guidelines. Visa clients can also use these guidelines to monitor the work by the QIRA. Visa will **NOT** accept forensic reports from non-approved forensic companies. QIRAs are required to release forensic reports and findings to Visa.

Note: The Visa client or compromised entity should contact the appropriate Visa region for a list of QIRAs.

Forensic investigations must be conducted using the following scope and methodology:

1. QIRA will assess compromised entity's computing environment to determine the scope of the forensic investigation and relevant sources of electronic evidence. This includes, but is not limited to:
 - Assessment of all external and internal connectivity points within each location involved.
 - Assessment of network access controls between compromised system(s) and adjacent and surrounding networks.

KEY POINT TO REMEMBER
Visa reserves the right to engage the QIRA.

2. QIRA will acquire electronic evidence from the compromised entity's host and network-based systems.
 - Forensic evidence acquisition must be conducted onsite at the compromised entity's premises.
 - If circumstances do not permit onsite evidence acquisition, QIRA must notify Visa.
 - Preservation of all potential electronic evidence on a platform suitable for review and analysis by a court of law, if applicable.
3. Forensically examine electronic evidence to find cardholder data and establish an understanding of how a compromise may have occurred.

4. Verify that cardholder data is no longer at risk and/or has been removed from the environment.
5. Verify that the compromised entity has contained the incident.
6. QIRA must use Visa's Incident Report template and provide a forensic report to all parties involved in the incident.
7. Perform external and internal vulnerability scans, including network and application scans.
8. The following actions must be included as part of the forensic investigation:
 - Determine and describe the type of processing environment:
 - Organization Description (check all that apply):
 - VisaNet processor
 - Issuer only
 - Acquirer only
 - Both issuer and acquirer
 - Pre-paid issuer
 - Third-party processor
 - Merchant
 - Other: _____
 - Estimated annual number of credit and or debit transactions for Visa-branded products (based on interview; exact numbers are not required):
 - Visa credit
 - Visa debit (Visa Signature only)
 - Visa with PIN (ATM with PIN)
 - Interlink (POS with PIN)
 - Plus (ATM with PIN)
 - Visa Prepaid (include list of Prepaid products)
 - Other: _____

9. Check and determine cardholder information that is at risk. This includes:
 - Number of and types of Visa/Plus/Interlink/Prepaid accounts at risk. Identify those stored and captured by malware (e.g., packet sniffer, key logger).
 - List of associated account information at risk:
 - Full magnetic-stripe data (e.g., Track 1 and 2)
 - PIN blocks and clear-text PINs. To identify potential presence of PIN blocks, also look for the PIN block format code field (see *Account Data Layout Format, Appendix E*, for more information).
 - CVV2
 - Account number
 - Expiration date
 - Other sensitive data elements (e.g., SSN, DOB)
 - Cardholder name
 - Cardholder address
 - Cardholder e-mail address
 - QIRA to examine all potential locations, including payment applications, to determine if full magnetic-stripe data, CVV2, and/or PIN blocks are stored (whether encrypted or unencrypted) on production, backups, tables, development, test, software engineer, and administrator's machines.
 - QIRA should also check volatile memory for cardholder data.
 - If malware was used to capture cardholder data, QIRA must review any malware output logs and validate whether cardholder data was captured and stored.
 - Other logs that must be reviewed include the following:
 - Server
 - Application
 - Transaction
 - Troubleshooting
 - Debug
 - Exception or error files
 - QIRA must provide account information to Visa (see *Requirements for Account Data Request*, page 15).

10. Determine time frame of accounts at risk. For example:
 - Determine how long accounts were stored on the system(s).
 - Determine the transaction date(s) of accounts stored on the system(s).
11. Perform incident validation and assessment. This includes:
 - Establishing how a compromise occurred.
 - Identifying the source of the compromise.
 - Window of system vulnerability. This is defined as the frame of time in which a weakness(s) in an operating system, application or network could be exploited by a threat to the time that weakness(s) is properly remediated.
 - Determining if any cryptographic keys have been exposed or compromised.
 - Reviewing the entire debit and/or credit processing environment to identify all compromised or affected systems; considering the e-commerce, corporate, test, development, production systems, VPN, modem, DSL, cable modem connections, and any third-party connections.
 - If applicable, review VisaNet endpoint security and determine risk.
 - Identifying the date(s) that account data was transferred out of the network by the intruder or malware.
 - Date(s) when the entity began using the payment application and version number. Determine if the payment application is PA-DSS compliant.
 - If available, identify the date(s) when the entity installed a patch or an upgrade to no longer retain prohibited data.
 - The date(s) that malware was installed on the system, if applicable.
 - Date(s) when malicious code, such as packet sniffer and/or key logger, was activated to capture payment card data on the network and system. QIRA must include date(s) of when malware was de-activated.
 - Determine the window of intrusion. This is the first confirmed date that the intruder or malware entered the system to the date of containment
12. Determine what applicable PCI security requirements apply:
 - PCI DSS
 - PCI PIN Security Requirements
 - PCI POS PIN Entry Device Security Requirements
 - PCI Encrypting PIN PAD (EPP) Security Requirements
 - PCI PA-DSS
13. If malware and bad IPs are identified in the compromise, the QIRA must submit the malware code and bad IPs via a secure distribution to *uscyberforensics@visa.com*.

Table of Entities and Requirements Applicability

REQUIREMENTS	TYPES OF ENTITIES						
	Issuer Processor	Acquirer Processor	Credit Only Merchant	Debit Accepting Merchant	Issuer and Acquirer Processor	ATM Processor	Third-Party Servicer
PCI DSS	Applies	Applies	Applies	Applies	Applies	Applies	Applies
PCI PIN Security Requirements	Applies if driving their own ATMs	Applies if processing debit	N/A	Applies	Applies	Applies	Applies if processing debit
PCI POS and PCI EPP PIN Entry Device Security Requirements	N/A	Applies if processing debit	N/A	Applies	Applies	Applies	Applies if processing debit
PCI PA-DSS	Applies	Applies	Applies	Applies	Applies	Applies	Applies

14. QIRAs must utilize Visa's report template. See *Appendices C and D, Incident Report template* for more information.

Appendix C: Preliminary Incident Report Template

This section contains the content and format standards that must be followed when completing a Preliminary Incident Response Report.

The Preliminary Incident Response Report document can be completed by the compromised entity or by an approved QIRA. Once completed, the report must be distributed to Visa, the client, and the compromised entity. Visa will classify the report as Visa Confidential.

QUESTIONS	RESPONSES
Name of compromised entity	
Date arrived onsite	
Evidence of a breach (Y/N)	
First confirmed date that the intruder or malware entered the network	
Scope of forensic investigation (e.g., single vs. numerous locations)	
Type of data impacted (e.g., full track, CVV2, PIN blocks)	
Window of system vulnerability	
Initial thoughts on attack vector	
Is the security breach ongoing or has it been contained?	
Other comments	

Appendix D: Final Incident Report Template

I. Executive Summary (include the following information):

- Date when the forensic company was engaged
- Date(s) when forensic investigation began
- Location(s) visited or forensically reviewed
- A brief summary of the scope of the forensic investigation
- A brief summary of the environment reviewed (details must be documented under the “Findings” section)
- Cause of intrusion
- Date(s) of intrusion
- Data elements at risk (e.g., full track, CVV2, PIN blocks)
- Specify whether or not the security breach has been contained

II. Background

- Brief summary of compromised entity company:
- Type of business entity:
 - Merchant (brick and mortar, e-commerce or both)
 - Prepaid issuer
 - Issuer
 - Acquirer
 - Acquirer processor
 - Issuer processor
 - ATM processor
 - Third-party service provider (web hosting; co-location)
 - Encryption Support Organization (ESO)
 - Payment application vendor
 - Payment application reseller

- PCI compliance and other information:
 - PCI DSS level and compliance status
 - Number of locations
 - Parent company (if applicable)
 - Franchise or corporate-owned

III. Incident Dashboard

CLIENT	TYPE OF BUSINESS ENTITY
Date when entity identified compromise	
Method of identification	Self Detection or Common Point of Purchase
Window of system vulnerability	
Window of intrusion	
Malware installation date(s), if applicable	
Date(s) of real time capture, if applicable	
Date(s) that data was transferred out of the network, if applicable	
Window of payment card data storage	
Transaction date(s) of stored accounts	
Date and version of POS installation(s), if applicable	
Type of data exposed	▪ Cardholder name ▪ Cardholder address ▪ PAN ▪ Expiry date ▪ CVV2 ▪ Track data ▪ Encrypted PINs
Brand exposure	▪ Visa ▪ MC ▪ DISC ▪ AMEX ▪ JCB

CLIENT	TYPE OF BUSINESS ENTITY
Number of cards exposed (both live system space and unallocated space)	▪ Include breakdown by card brand type ▪ Include breakdown of the following: - Signature - PIN-based transactions - Issuer-only data - Non-issuer data - Prepaid data
Logs that provided evidence: ▪ Firewall logs ▪ Intrusion detection systems ▪ Database queries ▪ FTP server logs ▪ System login records ▪ Web server logs	▪ File integrity monitoring output ▪ Transaction logs ▪ Remote access logs ▪ Wireless connection logs ▪ Anti-virus logs ▪ Security event logs ▪ File creation/access date
Suspected cause summary	Insert brief case summary. Detailed findings should be included in the "Findings" section of the report.

If applicable, document the type of cryptographic keys at risk. (See "*PIN Security Requirements*", page 46 of this section.)

ISSUER SIDE CRYPTOGRAPHIC KEYS	ACQUIRER SIDE CRYPTOGRAPHIC KEYS
Issuer Working Keys (IWK)	Acquirer Working Keys (AWK)
PIN Verification Keys (PVK)	POS, ATM, EPP PIN Encryption Keys
CVV, DCVV, ICSVV Verification Keys CVV2 Verification Keys (CVK2) Cardholder Authentication Verification Value Keys (CAVV and CAK) Cardholder Authentication Attempts Value Keys (CAAV)	POS, ATM, EPP Key Encrypting Keys (KEKs)
PIN Generation Keys	Remote Initialization Keys
Master Derivation Keys (MDK)	Host to Host Working Keys Key Encrypting Keys (KEKs)
Host to Host Working Keys Key Encrypting Keys (KEKs)	Switch Working Keys
Switch Working Keys	

IV. Network Infrastructure Overview

- Provide a diagram of the network that includes the following:
 - Cardholder data sent to central corporate server or data center
 - Upstream connections to third-party processors
 - Connections to Visa client bank networks
 - Remote access connections by third-party vendors or internal staff
 - Inbound/outbound network connectivity
 - Network security controls and components (network security zones, firewalls, hardware security modules, etc.)
 - Clearly identify all infrastructure components implemented or modified after the time frame of the compromise

V. Findings

- Provide specifics on firewall, infrastructure, host, and personnel findings
- Identify any and all changes made to the compromised entity's computing environment after the identification of a compromise
- Provide specific dates of network, system, or payment application changes
- Include any and all forensic evidence supporting changes made to networks, systems, and POS components
- Identify any data accessed by unauthorized user(s)

- Identify any data transferred out of the network by unauthorized user(s)
- Identify any evidence of data deletion from systems involved in a compromise
- If applicable, identify any deleted data recovered through forensic file recovery methods
- Identify any third-party payment applications, including version number
- Identify any upgrades/patches to the payment application that address removal of magnetic-stripe data, CVV2, and/or encrypted PIN blocks
- Provide an attack timeline of events. Include relevant date(s) and activities (e.g., date/time created, system/file evidence, description of evidence)
- Include a list of compromised systems/hosts (e.g., operating system; application and its functionality)
- Include a list of malicious IPs. Include any information related to malicious IPs (e.g., part of hacker group)
- Include a list of all malware identified. Include the following information on malware:
 - Name of malware
 - MD5 Hash
 - Registry settings
 - File size
 - System path

VI. Compromised Entity Containment Plan

- Document what the entity has done to contain the incident. Include date(s) of containment.

VII. Recommendation (s)

- List recommendations by priority level

VIII. PCI DSS Compliance Status

- Based on findings identified in the forensic investigation, indicate the compliance status for each of the 12 basic requirements under the PCI DSS
- Document the specific PCI DSS requirements and sub-requirements that contributed to the security breach

PCI DSS		
REQUIREMENTS	IN PLACE	NOT IN PLACE
BUILD AND MAINTAIN A SECURE NETWORK		
Requirement 1: Install and maintain a firewall configuration to protect cardholder data		
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
PROTECT CARDHOLDER DATA		
Requirement 3: Protect stored cardholder data		
Requirement 4: Encrypt transmission of cardholder data across open, public networks		
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM		
Requirement 5: Use and regularly update anti-virus software		
Requirement 6: Develop and maintain secure systems and applications		
IMPLEMENT STRONG ACCESS CONTROL MEASURES		
Requirement 7: Restrict access to cardholder data by business need-to-know		
Requirement 8: Assign a unique ID to each person with computer access		
Requirement 9: Restrict physical access to cardholder data		
REGULARLY MONITOR AND TEST NETWORKS		
Requirement 10: Track and monitor all access to network resources and cardholder data		
Requirement 11: Regularly test security systems and processes		
MAINTAIN AN INFORMATION SECURITY POLICY		
Requirement 12: Maintain a policy that addresses information security		

Appendix E: Account Data Layout Format

As mentioned in the previous section, clients are required to follow the following format on all account data requests. The account data must be **AUTHORIZATION DATA ONLY**.

Submitted data should be limited to one file. In cases where one file isn't possible, make every effort to minimize total file counts. If multiple files are provided, all of them must be consistent and contain the same formatting and transaction details.

The data submission may be a fixed width or delimited text file. Acceptable field delimiters are comma, tab, semicolon, space, or pipe (with or without text qualifiers). Field headers must be in the file or included on a separate file layout document.

Acceptable formats for each field (alpha (A), numeric (N), alphanumeric (AN), or alphanumeric special character (ANS)) are included in the descriptions. The International Standards Organization (ISO) field is noted if there is a corresponding field for further information.

The following are acceptable examples of file layouts and account data formats.

Advanced Format

In some cases, Visa will require additional transaction detail for further analysis. Provide information in as many fields as possible.

- Credit accounts signature (to include transaction details, see following bulleted list)
- Debit accounts signature (to include transaction details, see following bulleted list)
- Debit accounts used with a PIN (to include transaction details, see following bulleted list)
- Key-entered accounts (to include transaction details, see following bulleted list)

Transaction details are defined as follows:

- Primary account number (PAN)
- Expiration date
- Transaction amount
- Transaction date
- Merchant Category Code (MCC)
- Point-of-Service Entry Mode Code (POS entry)
- Visa Acquiring Bank Identification Number (BIN)

- Visa Acquiring Processor Control Record (PCR)
- Card Acceptor Identification Code (CAID)
- Card Acceptor Terminal Identification
- PIN transaction indicator
- Card acceptor name/location
- Card acceptor city
- Card acceptor country

Descriptions

Primary Account Number (PAN)

Format: N

ISO Field 2

The PAN contains the number identifying the cardholder account or relationship. The value is a cardholder account number of up to 19 numeric digits embossed on the card and also encoded on Track 1 and Track 2 of the magnetic stripe. The PAN is present in both face-to-face and card not present (CNP) transactions.

Allowable Card Account Number Lengths

Visa Card 16 digits.

16-digit example: 4444333322221111

Expiration Date

Format: N

ISO Field 7 (Track 1)

ISO Field 4 (Track 2)

Transaction Amount

Format: N

Cardholder transaction amount is in either U.S. dollars or per the currency code in Field 49. If the amount is not in U.S. dollars, then the currency code should also be present in a separate field.

Examples:

\$45.30

45.30

45.30, 250 (ISO currency code)

Transaction Date

Format: AN

Field contains the date of cardholder transaction. Acceptable formats should include the month, day, and year of transaction. Julian date is allowable.

Examples:

MM/DD/YYYY (03/15/2006)

DD/MM/YYYY (15/03/2006)

MM/DD/YY (03/15/06)

DD-MMM-YY (15-MAR-06)

March 15, 2006

YYDDD (06074) - Julian date

Merchant Category Code (MCC)

Format: N

ISO Field 18

Field contains a code describing the merchant's type of business product or service (also known as the Merchant Category Code (MCC)). Valid codes are listed in the *Visa U.S.A. Inc.* and *Visa International Operating Regulations*.

Examples:

5192 - Books, Periodicals, and Newspapers

5542 - Automated Fuel Dispensers

6011 - Financial Institutions - Automated Cash Disbursements

7230 - Hair Salon

Point-of-Service Entry Mode Code (POS entry)

Format: N

ISO Field 22: Positions 1 and 2 required

Field contains codes that identify the actual method used to capture the account number and expiration date and, when a point-of-transaction terminal is used, its PIN capture capability. This field is fixed-length with three sub-fields. The position assignments are as follows:

Positions 1 and 2

PAN and Date Entry Mode: A two-digit code that identifies the actual method used to enter the cardholder account number and card expiration date. This code specifies whether the entire magnetic stripe is included in an authorization or financial request.

Position 3

PIN Entry Capability – A one-digit code that identifies the capability of a terminal to accept PINs; it does not necessarily mean that the PIN was entered or is included in the message. A value of “1” means that the terminal can accept PINs; a value of “2” indicates that the terminal can not accept PINs.

Examples:

90 – Magnetic-stripe read and exact contents of Track 1 or Track 2 included. CVV or dCVV check is possible.

02 – Magnetic-stripe read; CVV checking may not be possible.

01 – Manual key entry

Visa Acquiring Bank Identification Number (BIN)

Format: N

This field identifies the financial institution acting as the acquirer of this customer transaction. The acquirer is the client or system user that signed the merchant, installed the ATM or ADM, or dispensed cash.

Visa BINs are six (6) digits. For processing centers handling multiple acquirers, this code identifies the individual acquirer or system user, not the overall processing center.

Examples:

400850

458307

Visa Acquiring Processor Control Record (“PCR”)

Format: N

This field, consisting of four (4) digits, identifies the processing center acting as the agent of the acquiring client that provides authorization, clearing, or settlement services for the merchant.

Examples:

4321 – ABC Processing Services

5678 – ABC Merchant

Card Acceptor Identification Code (CAID)

Format: ANS

ISO Field 42

This field contains the identifier of the card acceptor operating the point-of-sale or point-of-service (POS) terminal (or at the ATM) in local and in interchange environments. The CAID can be up to 15 bytes; if the ID is less than 15 positions, it must be left-justified and space-filled.

Examples:

140000015613401
58678062890003
6922I858RP357H
3655139M

Card Acceptor Terminal Identification

Format: ANS

ISO Field 41

This field contains a code that identifies the card acceptor terminal or ATM. For electronic POS terminals, when the ID is not unique to a specific terminal, Field 42 (CAID) can be used along with this field. ATM terminal IDs must be unique within the acquirer's network.

An identification code of fewer than eight (8) bytes must be left-justified and the remainder of the field space filled.

Examples:

80046578
8RNL9055
073
RI895B

PIN Transaction Indicator

Format: AN

This field indicates whether or not the transaction was PIN-based. This is the field that is used to differentiate signature-based versus PIN-based transactions.

Examples:

PIN, No PIN
Yes, No
Numeric codes: 1=PIN, 2=No PIN

Personal Identification Number (PIN) Data

ISO Field 52

Attributes: Fixed Length 8 bytes; 64-bit string/16 hex

Hex values include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Description: Field 52 contains an encrypted PIN block, formatted as a block of

16 hexadecimal digits. (0 – 9, A – F)

Examples:

```
2B9FFC29A40A25F3
9A40A252B9FFCBB1
40A2529A4077440A
BA669A40A2527229
2529A40A90ACD199
C510AE889FA92B7F
```

Security-Related Control Information

ISO Field 53

Attributes: Fixed Length 8 bytes; 16 numeric 4-bit BCD

Positions 5 – 6 PIN Block Format Code

The code in Field 53.3 (“PIN Block Format Code”) defines the format of Field 52 (“The PIN Block”). This field describes the PIN block format used by the acquirer/merchant and indicates the presence of a PIN. Values for Positions 5 – 6 are “01”, “02”, “03” and “04” and indicate the format of the PIN block used.

Note: Visa PIN block format numbering is different than that of ISO 9564, which is used in the PIN Security Requirements.

Card Acceptor Name/Location

Format: ANS

ISO Field 43

This field contains the name and location of the card acceptor (such as merchant or ATM) and includes the city name and country code. Field 43 has a single fixed length format, but the content of positions 1-25 depends on whether the request is for a Visa Interlink POS transaction, a Visa or Visa Plus ATM, or a VisaPhone transaction.

For Visa Interlink POS/ATM and Visa Plus ATM transactions, when the point of service is not in the same country as the acquirer, Field 43 must identify the card acceptor country. Field 43 also identifies the merchant or ATM location.

Positions 1-25, Card Acceptor Name:

POS: Merchants name as known to the cardholder.

ATM: The ATM location, branch number, or street address only (**Note:** the institution name is in Field 42).

Examples:

Bob's Fish Shack

AM RED CROSS DONATION

WWW MOULIN COM

Bookstore 53

Position 26-38, City Name:

POS: City where the customer transaction occurs.

Custom Payment Service (CPS) Card Not Present: Instead of the city name, these positions must contain the merchant's customer service telephone number, including country and area codes.

ATM: City where the ATM is located, branch number or street address only (**Note:** the institution name is in Field 42).

Examples:

Savannah

888 777 8888

PARIS

Madrid

Positions 39-40, Country Code:

POS and ATM: The two-character alpha code in uppercase format for the country where the cardholder transaction occurs or the ATM is located.

Examples:

US

FR

ES

PE

The following are samples of File Layouts:**Sample 1****File Layout**

Primary Account Number|Transaction Amount|Transaction Date|Merchant
Category Code|POS entry|Acquirer BIN|Acquirer PCR|Card Acceptor ID|Card
Acceptor Terminal ID|PIN Indicator|Card Acceptor Name|Card Acceptor
City|Card Acceptor Country

File

4111111111111111|87.5|06057|4816|01|426696|4008|426696100008681|1954
|N|GO MAN COM|BALTIMORE|US

4321432143214321|570.28|06068|5912|01|400088|9088|1420005995|05
995TSO|N|WALRUS|MT WHISKEY|US

4222222222222222|50|06066|7399|02|469216|2840|924944000192138||
N|J2 COMMUNICATE|323 850 3214|US

4141414141414141|11.89|06057|4816|01|400088|9088|106171000991232||
N|YABO VOICE|0821230270|EU

4564564564564568|174.5|06063|5399|01|400088|9088|000324202994
996|00110825|N|SOYLENT VENTURES|SUNNYTOWN|US

4987654321987654|1|06066|4814|01|461043|4401|67211400015P003|Q3
B50F0Q|N|UNICYCLE INTERNET|866 844 1849|US

4846512378945678|60.16|06056|4900|90|461043|8402|67354430019P0
03|Q3AAF40Q|Y|AQUILA INC|800 378 3357|US

4123456789123456|5.33|06058|7311|01|400088|9088|22628782|2468013
7|N|GOGGLE CC GOGGLE|OG ADWORDS|GB

**Sample 2 for
PIN Debit****File Layout (Debit Accepting Merchant)**

Primary Account Number|Transaction Amount|Transaction Date|Merchant
Category Code|POS entry|Acquirer BIN|Acquirer PCR|Card Acceptor ID|Card
Acceptor Terminal ID|PIN Entry Capability|Card Acceptor Name|Card Acceptor
City|Card Acceptor Country | PIN Block Format Code | PIN block

File

4111111111111111|87.5|06057|4816|01|426696|4008|426696100008681|1954
|1|GO MAN COM|BALTIMORE|US|01| 2B9FFC29A40A25F3

4321432143214321|570.28|06068|5912|01|400088|9088|1420005995|05
995TSO|1|WALRUS|MT WHISKEY|US|01| 9A40A252B9FFCBB1

4222222222222222|50|06066|7399|02|469216|2840|924944000192138||
 1|J2 COMMUNICATE|323 850 3214|US |01|40A2529A4077440A
 4141414141414141|11.89|06057|4816|01|400088|9088|106171000991232||1
 |YABO VOICE|0821230270|EU|01| BA669A40A2527229
 4564564564564568|174.5|06063|5399|01|400088|9088|000324202994
 996|00110825|1|SOYLENT VENTURES|SUNNYTOWN|US
 |01|2529A40A90ACD199
 4987654321987654|1|06066|4814|01|461043|4401|67211400015P003|Q3
 B50FOQ|1|UNICYCLE INTERNET|866 844 1849|US |01|C510AE889FA92B7F
 4846512378945678|60.16|06056|4900|90|461043|8402|67354430019P0
 03|Q3AAF40Q|1|AQUILA INC|800 378 3357|US |01|8A2527229C510AE8
 4123456789123456|5.33|06058|7311|01|400088|9088|22628782|2468013
 7|1|GOGGLE CC GOGGLE|OG ADWORDS|GB |01|9FA92B7FA2527229

Sample 3

File Layout

"PAN";"Transaction Amount";"Transaction Date";"MCC";"POS entry";"Acq
 BIN";"Acq PCR";"CAID";"CA Terminal ID";"PIN Indicator";"CA Name";"CA
 City";"CA Country"

File

"4111111111111111";"87.5";"06057";"4816";"01";"426696";"4008";"426696100
 008681";"1954";"N";"GO MAN COM";"BALTIMORE";"US"
 "4321432143214321";"570.28";"06068";"5912";"01";"400088";"9088";"142
 0005995";"05995TS0";"N";"WALRUS";"MT WHISKEY";"US"
 "4222222222222222";"50";"06066";"7399";"02";"469216";"2840";"92494
 4000192138";"N";"J2 COMMUNICATE";"323 850 3214";"US"
 "4141414141414141";"11.89";"06057";"4816";"01";"400088";"9088";"106171
 000991232";"N";"YABO VOICE";"0821230270";"EU"
 "4564564564564568";"174.5";"06063";"5399";"01";"400088";"9088";"00
 0324202994996";"00110825";"N";"SOYLENT
 VENTURES";"SUNNYTOWN";"US"
 "4987654321987654";"1";"06066";"4814";"01";"461043";"4401";"67211400
 015P003";"Q3B50FOQ";"N";"UNICYCLE INTERNET";"866 844 1849";"US"
 "4846512378945678";"60.16";"06056";"4900";"90";"461043";"8402";"673
 54430019P003";"Q3AAF40Q";"Y";"AQUILA INC";"800 378 3357";"US"
 "4123456789123456";"5.33";"06058";"7311";"01";"400088";"9088";"22628
 782";"24680137";"N";"GOGGLE CC GOGGLE";"OG ADWORDS";"GB"

Sample 4**File Layout**

Primary Account Number, Amount, Date, Merchant Category Code, POS entry, Acquirer BIN, Acquirer PCR, Card Acceptor ID, Card Acceptor Terminal ID, PIN Transaction ID, Card Acceptor Name, Card Acceptor City, Card Acceptor Country

File

```
4111111111111111,87.5,06057,4816,01,426696,4008,426696100008681,1954,
N,GO MAN COM,BALTIMORE,US
4321432143214321,570.28,06068,5912,01,400088,9088,1420005995,059
95TSO,N,WALRUS,MT WHISKEY,US
4222222222222222,50,06066,7399,02,469216,2840,924944000192138,,
N,J2 COMMUNICATE,323 850 3214,US
4141414141414141,11.89,06057,4816,01,400088,9088,106171000991232,,N,
YABO VOICE,0821230270,EU
4564564564564568,174.5,06063,5399,01,400088,9088,000324202994
996,00110825,N,SOYLENT VENTURES,SUNNYTOWN,US
4987654321987654,1,06066,4814,01,461043,4401,67211400015P003,Q3B
50FOQ,N,UNICYCLE INTERNET,866 844 1849,US
4846512378945678,60.16,06056,4900,90,461043,8402,67354430019PO
03,Q3AAF40Q,Y,AQUILA INC,800 378 3357,US
4123456789123456,5.33,06058,7311,01,400088,9088,22628782,2468013
7,N,GOGGLE CC GOGGLE,OG ADWORDS,GB
```

Sample 5**File Layout**

Field Name, Field Length

Primary Account Number, 19

Transaction Amount, 25

Transaction Date, 25

Merchant Category Code, 4

POS Entry Mode, 2

Acquirer BIN, 6

Acquirer PCR, 4

Card Acceptor ID, 15

Card Acceptor Terminal ID, 8

PIN Transaction ID, 1

Card Acceptor Name, 25

Card Acceptor City, 15

Card Acceptor Country, 2

File

4111111111111111 87.5 06057 48160142669640084266961000086811954
NGO MAN COM BALTIMORE US
4321432143214321 570.28 06068 59120140008890881420005995
05995TS0NWALRUS MT WHISKEY US
4222222222222222 50 06066 7399024692162840924944000192138
NJ2 COMMUNICATE 323 850 3214 US
4141414141414141 11.89 06057 4816014000889088106171000991232
NYABO VOICE 0821230270 EU
4564564564564568 174.5 06063
539901400088908800032420299499600110825NSOYLENT VENTURES
SUNNYTOWN US
4987654321987654 1 06066
481401461043440167211400015P003Q3B50F0QNUNICYCLE INTERNET
866 844 1849 US
4846512378945678 60.16 06056
490090461043840267354430019P003Q3AAF40QYAQUILA INC 800
378 3357 US
4123456789123456 5.33 06058 731101400088908822628782
24680137NGOGGLE CC GOGGLE OG ADWOR

Appendix F: PIN Security Requirements

PCI PIN SECURITY REQUIREMENTS			
OBJECTIVE 1			
PINs used in transactions governed by these requirements are processed using equipment and methodologies to ensure that they are kept secure.			
1. All cardholder-entered PINs are processed in equipment that conforms to the requirements for Tamper-Resistant Security Modules (TRSMs). TRSMs are considered tamper responsive or physically secure devices (i.e., penetration of the device will cause immediate erasure of all PINs, secret and private cryptographic keys, and all useful residues of PINs and keys contained within it).	YES ☐	NO ☐	N/A ☐
All newly deployed ATMs and POS PIN acceptance devices are compliant with the applicable PCI PIN Entry Device and Encrypting PIN Pad Security Requirements.			
2a. All cardholder PINs processed online are encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards. Any cryptographic technique implemented meets or exceeds the cryptographic strength of TDEA using double length keys.	YES ☐	NO ☐	N/A ☐
2b. All cardholder PINs processed offline using IC Card technology must be protected in accordance with the requirements in Book 2 of the <i>EMV IC Card Specifications for Payment Systems</i> and ISO 9564.	YES ☐	NO ☐	N/A ☐
3. For online interchange transactions, PINs are only encrypted using ISO 9564-1 PIN block formats 0, 1 or 3. Format 2 must be used for PINs that are submitted from the IC card reader to the IC card.	YES ☐	NO ☐	N/A ☐
4. PINs are not stored except as part of a store-and-forward transaction, and only for the minimum time necessary. If a transaction is logged, the encrypted PIN block must be masked or deleted from the record before it is logged.	YES ☐	NO ☐	N/A ☐

OBJECTIVE 2

Cryptographic keys used for PIN encryption/decryption and related key management are created using processes to ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.

5.	All keys and key components are generated using an approved random or pseudo-random process.	YES ☐	NO ☐	N/A ☐
6.	Compromise of the key-generation process is not possible without collusion between at least two trusted individuals.	YES ☐	NO ☐	N/A ☐
7.	Documented procedures exist and are demonstrably in use for all key-generation processing.	YES ☐	NO ☐	N/A ☐

OBJECTIVE 3

Keys are conveyed or transmitted in a secure manner.

8.	Secret or private keys are transferred by:	YES ☐	NO ☐	N/A ☐
	a. Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, TRSM) using different communication channels, or			
	b. Transmitting the key in ciphertext form			
	Note: Public keys must be conveyed in a manner that protects their integrity and authenticity.			
9.	Any single unencrypted key component is at all times during its transmission, conveyance, or movement between any two organizational entities:	YES ☐	NO ☐	N/A ☐
	a. Under the continuous supervision of a person with authorized access to this component, or			
	b. Locked in a security container (including tamper-evident packaging) in such a way that it can be obtained only by a person with authorized access to it, or			
	c. In a physically secure TRSM			
10.	All key encryption keys used to transmit or convey other cryptographic keys are (at least) as strong as any key transmitted or conveyed.	YES ☐	NO ☐	N/A ☐
11.	Documented procedures exist and are demonstrably in use for all key transmission and conveyance processing.	YES ☐	NO ☐	N/A ☐

OBJECTIVE 4**Key loading to hosts and PIN entry devices is handled in a secure manner.**

12. Unencrypted keys are entered into host Hardware Security Modules (HSMs) and PIN Entry Devices (PEDs) using the principles of dual control and split knowledge.	YES ☐	NO ☐	N/A ☐
13. The mechanisms used to load keys (such as terminals, external PIN pads, key guns, or similar devices and methods) are protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.	YES ☐	NO ☐	N/A ☐
14. All hardware and passwords used for key loading are managed under dual control.	YES ☐	NO ☐	N/A ☐
15. The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.	YES ☐	NO ☐	N/A ☐
16. Documented procedures exist and are demonstrably in use (including audit trails) for all key-loading activities.	YES ☐	NO ☐	N/A ☐

OBJECTIVE 5**Keys are used in a manner that prevents or detects their unauthorized usage.**

17. Unique secret cryptographic keys must be in use for each identifiable link between host computer systems.	YES ☐	NO ☐	N/A ☐
18. Procedures exist to prevent or detect the unauthorized substitution (i.e., unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.	YES ☐	NO ☐	N/A ☐
19. Cryptographic keys are only used for their sole intended purpose and are never shared between production and test systems.	YES ☐	NO ☐	N/A ☐
20. All secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal (i.e., PED) that processes PINs must be unique (except by chance) to that device.	YES ☐	NO ☐	N/A ☐

OBJECTIVE 6**Keys are administered in a secure manner.**

21. Keys used for enciphering PIN encryption keys (or for PIN encryption) must never exist outside of TRSMs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.	YES ☐	NO ☐	N/A ☐
22. Procedures exist and are demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) to a value not feasibly related to the original key.	YES ☐	NO ☐	N/A ☐
23. Key variants are only used in devices that possess the original key. Key variants are not used at different levels of the key hierarchy (e.g., a variant of a key encipherment key used for key exchange cannot be used as a working key or as a master file key for local storage).	YES ☐	NO ☐	N/A ☐
24. Secret and private keys and key components that are no longer used or have been replaced are securely destroyed.	YES ☐	NO ☐	N/A ☐
25. Access to secret and private cryptographic keys and key materials must be limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.	YES ☐	NO ☐	N/A ☐
26. Logs are kept for any time that keys, key components, or related materials are removed from storage or loaded to a TRSM.	YES ☐	NO ☐	N/A ☐
27. Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.	YES ☐	NO ☐	N/A ☐
28. Documented procedures exist and are demonstrably in use for all key administration operations.	YES ☐	NO ☐	N/A ☐

OBJECTIVE 7**Equipment used to process PINs and keys is managed in a secure manner.**

29. PIN-processing equipment (PEDs and HSMs) is placed into service only if there is assurance that the equipment has not been substituted or made subject to unauthorized modifications or tampering prior to the loading of cryptographic keys.	YES ☐	NO ☐	N/A ☐
30. Procedures exist that ensure the destruction of all cryptographic keys and any PINs or other PIN-related information within any cryptographic devices removed from service.	YES ☐	NO ☐	N/A ☐
31. Any TRSM that is capable of encrypting a key and producing cryptograms of that key is protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of either or both of the following: a. Dual access controls are required to enable the key encryption function. b. Physical protection of the equipment (e.g., locked access to it) under dual control.	YES ☐	NO ☐	N/A ☐
32. Documented procedures exist and are demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., PEDs and HSMs) placed into service, initialized, deployed, used, and decommissioned.	YES ☐	NO ☐	N/A ☐

Appendix G: List of Supporting Documents

The following documents can be downloaded at www.visa.com/cisp, www.visa.com/pinsecurity, www.visa.com/pin, www.pcisecuritystandards.org

- Qualified CISP Incident Response Assessor (QIRA) List – List of forensic companies qualified to perform a PCI forensic investigation on compromised entities.
- Qualified PCI Assessor (QSA) - List of assessors qualified to perform PCI assessments for those entities requiring onsite validation of PCI compliance.
- PCI Data Security Standard (PCI DSS) – Detailed security requirements to which Visa clients, merchants, and service providers must adhere to ensure the protection of cardholder data.
- PCI Security Audit Procedures – Detailed security requirements, guidelines, and testing procedures to assist a PCI QSA in verifying that an entity is in compliance with the PCI DSS.
- PCI Self-Assessment Questionnaire (SAQ) - The PCI SAQ is an important validation tool primarily used by smaller merchants and service providers to demonstrate compliance to the PCI DSS. Responses must address any system(s) or system component(s) involved in processing, storing, or transmitting Visa cardholder data. **Note:** For any answers where N/A is marked, a brief explanation should be attached.
- PCI Security Scanning Procedures - Procedures and guidelines for conducting network security scans for entities and third-party service providers who are scanning their infrastructures to demonstrate compliance to the PCI DSS.
- Acquiring institutions and agents involved with PIN transaction processing must comply with the security requirements and guidelines specified in the PIN Security documents that can be downloaded from www.visa.com/pinsecurity.
- PCI PIN Security Requirements (visit www.visa.com/pinsecurity).
- Visa PIN Security Program Auditor's Guide (visit www.visa.com/pinsecurity).

Appendix H: Glossary of Terms

802.11	IEEE 802.11 is a set of standards for wireless local area network (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum bands.
Acquirer	Financial institution that enters into agreements with merchants to accept Visa cards as payment for goods and services. Commonly referred to as the “merchant bank”.
Agent	Any contractor, including third-party processors and servicers, whether a client or non-client, engaged by a client to provide services or act on its behalf in connection with Visa payment services.
At Risk Accounts	Refers to accounts that were included in a CAMS “Alert” of a suspected or confirmed compromised event.
Authentication	The process of verifying the true origin or nature of the sender and/or the integrity of the text of a message.
Authorization	A process by which an issuer approves a transaction for a specified amount with a merchant.
Backdoor	A method of bypassing normal authentication and obtaining access to plaintext information while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice), or could be a modification to an existing program or hardware device.
Bank Identification Number (BIN)	A unique number assigned by the bankcard association to its members. On a cardholder’s account number, the BIN appears as the first six digits. Visa BINs begin with the number “4.”
Card Authorization Acceptor ID	Information found in the authorization message (Field 42) from a legitimate transaction at the Acceptor ID CPP-identified merchant.
Card Not Present	A merchant, market, or sales environment where transactions occur without a valid Visa card being present. “Card not present” is used to refer to mail order/telephone order merchants and sales environments, as well as the Internet.
Card Present	A merchant, market, or sales environment in which a transaction can be completed only if both a valid Visa card and the cardholder are present and the sale is processed by an individual representing the merchant or the acquirer. Card present transactions include face-to-face retail sales and cash disbursements.

Common Point of Purchase (CPP)	Refers to the location of a legitimate transaction (usually a purchase or cash advance transaction) common to a number of accounts involved in a fraud scheme of similar character. The “common point of purchase” is assumed to be the point of compromise.
Card Verification Value (CVV)	A unique three-digit “check number” encoded on the magnetic stripe of all valid cards. The number is calculated by applying an algorithm (a mathematical formula) to the stripe-encoded account information, and is verified online at the same time that a transaction is authorized.
Card Verification Value 2 (CVV2)	A Visa fraud prevention system used in card-not-present transactions to ensure that the card is valid. The CVV2 is the three-digit value that is printed on the back of all Visa cards. Card-not-present merchants ask the customer for the CVV2 and submit it as part of their authorization request. For information security purposes, merchants are prohibited from storing CVV2 data.
Cardholder	The person or entity whose name is embossed on the face of a card or encoded on the magnetic stripe.
Cardholder Data	All identifiable personal data about the cardholder and the relationship to the client (e.g., account number, expiration date, data provided by the client, other electronic data gathered by the merchant/agent). This term also applies to other personal insights gathered about the cardholder such as address, telephone number, etc.
Client	An organization that is a member of Visa and issues cards and/or signs merchants.
Compromise	Process that exposes cardholder account information to third parties, placing cardholders at risk of fraudulent use.
Compromised Account	Accounts downloaded by an intruder or found in criminal possession.
Compromised Account Management System (CAMS)	Via CAMS, acquirers, merchants and law enforcement officers can safely upload compromised and stolen/recovered accounts directly to Visa. As this information is received by CAMS, e-mail alert messages are automatically sent to registered issuer users to notify them of the compromised and stolen/recovered accounts.
Cryptographic Key	A parameter used in conjunction with a cryptographic algorithm that determines: ▪ The transformation of plaintext data into ciphertext data ▪ The transformation of ciphertext data into plaintext data ▪ A digital signature computed from data ▪ The verification of a digital signature computed from data ▪ An authentication code computed from data or ▪ An exchange agreement of a shared secret
Denial of Service (DoS)	Denial of Service (DoS) is a tool or program used by intruders to cause networks and/or computers to cease operating effectively or to erase critical programs running on the system.

Electronic Commerce (e-commerce)	The purchase of goods and services over the Internet without a paper transaction between buyer and seller.
Entity	An organization that stores, processes or transmits account information. Typically the victim in a compromise. Also refers to any payment industry organization that must be PCI DSS compliant.
Encryption	An online data security method that scrambles data so that it is difficult to interpret without a corresponding decryption key.
Event	Refers to a single event of a known or suspected data compromise. It is used interchangeably with the term “incident”.
Full-Track Data	There are two tracks of data on a bankcard’s magnetic stripe: ▪ Track 1 is 79 characters in length. It is alphanumeric and contains the account number, the cardholder name, and the additional data listed on Track 2.. ▪ Track 2 is the most widely read. It is 40 characters in length and is strictly numeric. This track contains the account number, expiration date, secure code, and discretionary institution data.
Hacker	A person who deliberately logs on to other computers by circumventing the log-on security system. This is sometimes done to steal valuable information or to cause damage that might be irreparable.
IEEE (Institute of Electrical and Electronics Engineers, Inc.)	The Institute of Electrical and Electronics Engineers, Inc., is an international non-profit, professional organization for the advancement of technology. More info at www.ieee.org .
Incident	Refers to each single occurrence of known or suspected data compromise. It is used interchangeably with the term “event”.
Incident Response Managers	Visa staff designated by a regional office to coordinate response to incidents.
Issuer	A financial institution that issues Visa products.
Magnetic Stripe (Mag Stripe)	A strip of magnetic tape located on the back of all bankcards. The magnetic stripe is encoded with identifying account information as specified in the Visa Operating Regulations. On a valid card, the account information on the magnetic stripe matches similar embossed information located on the front of the card.
Man-in-the-Middle (MITM)	A form of eavesdropping in which an attacker makes independent connections with the victims and relays messages between them, making the victims believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.

MD5 Hash	The MD5 hash (also known as checksum) for a file is a 128-bit value, similar to taking a fingerprint of a file.
Member	An organization that is a member of Visa and issues Visa cards and/or acquires merchant transactions.
Merchant	An entity that enters into a card acceptance agreement with a Visa acquirer or processor.
Merchant Bank	See Acquirer.
Merchant Level	All merchants fall into one of four merchant levels based on Visa transaction volume over a 12-month period.
PAN	Primary Account Number.
Payment Card Industry Data Security Standard (PCI DSS)	A set of requirements established by the payment card industry to protect cardholder data. These requirements apply to all members, merchants, and service providers that store, process, or transmit cardholder data.
Payment Card Industry (PCI) PIN Security Requirements	A comprehensive set of measures created for the safe transmission and processing of cardholder PINs during ATM and point-of sale (POS) PIN-entry device (PED) transactions. All participants in the payment processing chain that manage cardholder PINs and encryption keys must be in full compliance with the PCI PIN Security Requirements. This document can be downloaded from the PIN website at www.visa.com/pinsecurity .
PCI Security Standards Council ("PCI SSC")	The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including: the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and Pin-Entry Device (PED) Requirements.. For more information on PCI SSC, visit www.pcisecuritystandards.org/ .
Personal Identification Number (PIN)	An alphabetic and/or numeric code which may be used as a means of cardholder identification
Point of Compromise (POC)	Refers to the location where account number data was obtained by unauthorized third parties.
Qualified CISP Incident Response Assessor (QIRA)	Visa-approved security vendors who perform forensic investigations in the event of a security incident. A list of QIRAs can be obtained at www.visa.com/cisp .

Qualified Data Security Company (QDSC)	A security company qualified by the PCI SSC to perform a PCI Data Security Assessment according to the PCI Security Audit Procedures. Please visit the PCI Security Standards Council website (www.pcisecuritystandards.org) for details on the PCI program requirements.
Rootkit	A program designed to take administrative control of a computer system without authorization from the system's owners.
Secure Shell (SSH)	"Secure Shell" is a network protocol that allows data to be exchanged using a secure channel.
Service Set Identifier (SSID)	"Service Set Identifier" is the name used to identify the particular 802.11 wireless LAN to which a user wants to attach.
Telnet (Telecommunications Network)	A network protocol used on the Internet or on Local Area Network (LAN) connections.
Third-Party Processor	A service provider organization acting as the client's agent to provide authorization, clearing, or settlement services for merchants and members.
Third-Party Servicer	A service provider organization that is not a client of Visa and is not directly connected to VisaNet, but provides the following services to the client: Response processing for Visa program solicitations Transaction processing (including gateways) Data capture Other administrative functions such as chargeback processing, risk/security reporting, and customer service
Visa Cardholder Information Security Program (CISP)	A Visa program that establishes data security standards, procedures, and tools for all entities (merchants, service providers, issuers, and merchant banks) that store Visa cardholder account information. CISP compliance is mandatory. CISP requirements prohibit merchants and service providers from storing the full contents of any magnetic stripe, CVV2, or PIN-block data. For more information regarding CISP, visit www.visa.com/cisp .
VisaNet	The data processing systems, networks and operations used to support and deliver authorization services, exception file services, clearing and settlement services and any other services.
WAP (Wireless Application Protocol)	An open international standard for application layer network communications in a wireless communication environment.

WAP or AP (Wireless Access Point)	A computer networking device that allows wireless communication devices to connect to a wireless network using Wi-Fi and related standards. The WAP usually connects to a wired network and can relay data between both wireless and wired devices (such as computers or printers) on the network.
WEP (Wired Equivalent Privacy)	An algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio and are more susceptible to eavesdropping than wired networks.

Appendix I: Investigation Definitions

TERMINOLOGY	DESCRIPTION
Date(s) that data was transferred out of the network	The confirmed date(s) that data was transferred out of the network by the intruder or malware.
Date and Version of POS Installation (s)	Date(s) of when the entity began using the POS application and version number. If available, include date(s) of when entity installed a patch or an upgrade to no longer retain prohibited data.
Malware Installation Date(s)	The date(s) that malware was installed on the system, if applicable.
Date(s) of Real-Time Capture	Date(s) of when malicious code/malware, such as packet sniffer and/or key logger, was activated to capture payment card data on the network and system. Should also include date(s) of when malware was de-activated.
Window of Intrusion	First confirmed date that intruder or malware entered the system to the date of containment. Examples of containment include, but not limited to: ▪ Removal of malware or rebuilt of compromised systems ▪ Compromised system removed from the network ▪ Blocking of malicious IPs on the firewall ▪ Rotation of compromised passwords
Window of Storage	"Window of Storage" is defined as the frame of time in which a given set of prohibited data is initially placed on a system to the time that same data was removed. It answers the question, "how long was the given set of data stored?"
Transaction date(s) of stored accounts	Transaction date(s) is defined as the date of the transactions stored on the system.
Window of System Vulnerability	"Window of Vulnerability" is defined as the frame of time in which a weakness in an operating system, application or network could be exploited by a threat to the time that weakness is properly remediated. It answers the question, "how long was the system at risk to a given compromise?" Overall time period that a system was vulnerable to attack due to system weaknesses. For example, lack of/or poorly configured firewall, missing security patches, insecure remote access configuration, default passwords to POS systems, insecure wireless configuration.

Appendix J: Secret Service Electronic Crimes Task Force (ECTF)

New England Electronic Crimes Task Force

(617) 565-6640

Metro-Charlotte Electronic/Financial Crimes Task Force

(704) 442-8370

Chicago Electronic Crimes Task Force (CECTF)

(312) 353-5431

Cleveland Electronic Crimes Task Force

(216) 706-4365

Dallas N-Tec Electronic Crimes Task Force

(972) 868-3200

Houston HITEC Electronic Crimes Task Force

(713) 868-2299

Las Vegas Electronic Crimes Task Force

(702) 388-6571

Los Angeles Electronic Crimes Task Force

(213) 533-4650

Miami Electronic Crimes Task Force

(305) 863-5000

New York Electronic Crimes Task Force

(718) 625-7135

San Francisco Bay Area Electronic Crimes Task Force

(415) 744-9026

South Carolina Electronic Crimes Task Force

(803) 772-4015

Washington -Metro Electronic Crimes Task Force

(202) 406-8000

For Further Information:

www.ectaskforce.org or

www.secretservice.gov

(305) 863-5000

Appendix K: Federal Bureau of Investigations (FBI)

Infragard at www.infragard.net

FBI at www.fbi.gov

ATTACHMENT "D"
CERTIFICATION
DISBURSEMENT OF PREVIOUS PAYMENTS

Date: _____, 200__

Contract No.: _____

Financial Project No. 423249-1-32-01

Contract For: Payment Card Industry (PCI) Services

To release payment for all work performed in the Month of _____ 200__

(State)

(Zip)

As prime contractor for the above referenced contract, hereby certifies that all subcontractors, laborers, and material suppliers having an interest in this contract have received their pro rata share of all previous payments made by the Department for all work completed and materials and equipment furnished in the previous period.

(Name of Business)

(Signature) Owner, President, or Designated Officer (Corp. Resolution)*

(Address)

(Print/Type Name)

(City)

(Title)

*If person signing for the Business is someone other than the Owner, or President, a copy of the Corporate Resolution granting signature authorization must be attached to form.

CERTIFICATION MUST BE ATTACHED TO INVOICE

ATTACHMENT "E"

STATE OF FLORIDA DEPARTMENT OF TRANSPORTATION
CERTIFICATE OF CONTRACT COMPLETION

Contract Number _____

FPI Nos. 423249-1-32-01

Project Description _____

Contractor _____

Contract For: Payment Card Industry (PCI) Services

Contract Date _____ Total Amount \$ _____

CONTRACTOR'S AFFIDAVIT

I solemnly swear and affirm: That the work under the above named contract and all amendments and supplements thereto have been completed in accordance with the requirements of said contract; that all costs incurred for equipment, materials, labor, and services against the project have been paid; that no liens have been attached against the project; that no suits are pending by reason of work on the project under the contract; that all Worker's Compensation claims are covered by Worker's Compensation insurance as required by law; that all public liability claims are adequately covered by insurance, and that the Contractor shall save, protect, defend, indemnify, and hold the Owners harmless from and against any and all claims which arise as a direct or indirect result of any transaction, event or occurrence related to performance of the work contemplated under said contract.

(Signature), Owner, President or other Designated Officer (Corp. Resolution)

(Title)

(Corporate Seal)

STATE OF _____

COUNTY OF _____

The foregoing affidavit was acknowledged before me this _____ day of _____, 200__

by _____, on behalf of the Contractor. He/She is personally known to me or has
(Print / Type Name of Person Signing Above)

produced _____, as identification.
(Type of Identification)

Notary Public: _____
(Signature)

(Notary Stamp)

Type/Print Name: _____

* If person signing for the Business is someone other than the Owner or President, a copy of the Corporate Resolution granting signature authorization must be furnished in the bid package.

CERTIFICATION MUST BE ATTACHED TO THE FINAL INVOICE

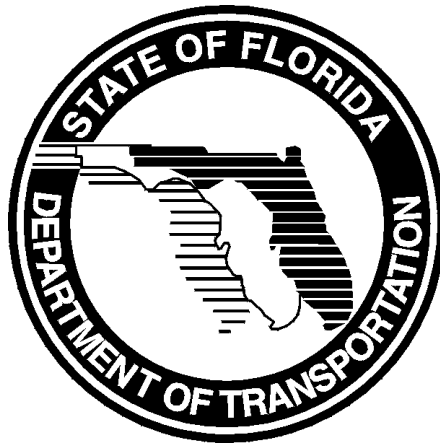


EXHIBIT "B"

METHOD OF COMPENSATION

RFP-DOT- 09/10-8001-KB

PAYMENT CARD INDUSTRY (PCI) SERVICES

FPI No. 423249-1-32-01

EXHIBIT B
METHOD OF COMPENSATION
PAYMENT CARD INDUSTRY (PCI) SERVICES

1.0 PURPOSE:

This Exhibit defines the limits and method of compensation to be made to the Vendor for services set forth in Exhibit "A" and the method by which payments shall be made.

2.0 COMPENSATION

For the satisfactory **performance** of the services detailed in Exhibit "A", the Vendor shall be paid a Lump Sum Amount of \$_____.

\$ _____	from Department Fiscal Year 2009-2010
\$ _____	from Department Fiscal Year 2010-2011
\$ _____	from Department Fiscal Year 2011-2012

Legislative appropriations are on a fiscal year basis. The Department's fiscal year begins July 1st of each year and ends on June 30th of each succeeding year.

Upon execution of this Agreement, the Department gives notice to the Vendor that the amount shown above for Fiscal Year 2009-2010 is available to have the Vendor render services. The Department and the Vendor acknowledge and agree that funding for the amounts shown above for fiscal year(s) subsequent to Fiscal Year 2009-2010 are contingent upon an annual appropriation by the Legislature and that until such appropriation, the Vendor shall not render services. The Department shall provide the Vendor a written notice if legislative funding for the fiscal year(s) subsequent to Fiscal Year 2009-2010 are not made available.

The Department and the Vendor acknowledge and agree that the Vendor shall not provide services or incur costs during a fiscal year which would result in exceeding the funding established for the Fiscal Year nor shall the Department be obligated to reimburse the Vendor for services or costs which would result in exceeding the funding established for a fiscal year. The Department, based on need and availability, may increase or decrease funding for a given fiscal year by Amendment.

3.0 BASIS OF PAYMENT

The Department agrees to pay the Vendor for the services performed, an amount of compensation and method of payment as described and detailed herein and in Exhibit "C", Price Proposal.

3.1 Payment Card Industry (PCI) Services 1 Merchant and Business Impact Analysis (BIA):

Payment for this activity shall constitute full compensation for all annual PCI services that will be required for an annual passing report of compliance, Exhibit "A", Section 4.0 through 4.6.5. Payment will be made on the basis of the contract lump sum price as shown in Exhibit "C", under the Pay Item No. 1.

3.2 Additional Services:

Hourly PCI Audit Services (remediation consulting) - Payment for this activity shall constitute full compensation for services provided beyond the minimum PCI Data Security Standards (DSS). Payment for this activity will be made at the contract unit price as shown in Exhibit "C", Price Proposal under Pay Item No. 2.

Forensic Security Services- Payment for this activity shall constitute full compensation for required forensic services as specified in Exhibit "A", Section 4.5. Payment will be made on the basis of the contract unit prices as shown in Exhibit "C",

4.0 INVOICING

- A. Payment will be made following receipt and approval of a monthly invoice package for all work performed and accepted by the Department's contract manager. The invoice package shall include an itemized monthly invoice and all contract maintenance work documents, as specified in item B and C immediately below. The Vendor's monthly invoice package shall be submitted to the Department's contract manager by no later than the 15th of each month. **Failure to submit timely invoices could affect Vendor's performance rating.**

The Vendor's invoice package shall be submitted to the address below.

Department of Transportation
Turnpike SunPass Service Center
7941 Glades Road
Boca Raton, Florida 33434
Attention: Rodney Patterson
Phone 561-488-5371

- B. The itemized monthly invoice shall be a legible summary on the Vendor's letterhead that includes the following:

1. Remittance Address
2. List of Contract Maintenance Work Document Number(s)
3. Total amount of invoice
4. Current Contract Balance
5. State Contract Number
6. State Financial Project Identification Number
7. Total Labor Hours

8. Billing period
 9. Total Quantity and amount for each pay item
- C. A contract maintenance work document for all authorized work must be provided. The contract maintenance work document shall include the following:
1. Date of Completion
 2. Estimated Quantity for each pay item
 3. Actual Quantity for each pay item
 4. Total amount for each work document
 5. Description of actual work performed
 6. Location of work
 7. Copies of all receipts for parts purchased must be attached
- D. The "LABOR HOURS" are the total number of expended hours times the number of employees assigned to perform the work. The information is required for entry into the Department's Maintenance Management System (MMS) only, and not intended as a basis of payment.
- 4.3 The Vendor shall provide a statement, with all but the first pay request, to the Department which certifies that the Vendor has disbursed to all sub-vendors, laborers, and materials suppliers, having an interest in the contract, their pro-rata shares of the payment, out of the previous payments received by the Vendor for all work completed and materials furnished in the previous period. This certification shall be in the form designated by the Department (see Attachment "C", Disbursement of Previous Payments). The Department shall not make any payments after the initial payment until the Vendor furnishes said certification, unless the Vendor demonstrates good cause for not making any such required payment and provides written notification of any such good cause to both the Department and the affected sub-vendors, laborers, and material suppliers.
- 4.4 The cost of any repairs performed by the Department as a result of the Vendor's performance of duties or employees shall be deducted from the Vendor's monthly payment. The Department also reserves the right to withhold and/or deny payment for the Vendor's performance of duties or employees shall be deducted from the Vendor's monthly payment.
- 4.5 The Department reserves the right to withhold the payment or partial payment of the Vendor's invoice and/or deny payment to the Vendor when, in the opinion of the Department's Contract Manager, less than the services listed on the invoice were performed or services were inadequate, not authorized, or not actually performed.
- 4.6 No compensation shall be paid separately for travel time, expenses or tolls. Therefore, all the anticipated travel time and travel expenses incurred by the Vendor shall be included in the Vendor's unit prices. This should also include charges for the use of Florida's Turnpike. The Vendor and any subcontractor shall pay toll charges for all vehicles and equipment at the standard rate applicable to the general public.
- 4.7 The Vendor shall submit all the outstanding invoices or issues pertaining to the contract within forty-five (45) calendar days of the termination date/last day of the term of the contract. Failure to timely submit the outstanding invoices or issues, by the Vendor, may be grounds for the Department to close

the contract. The Department shall not be obligated to reimburse the Vendor for any invoice submitted thereafter unless the Vendor has obtained a written exception to the time limit from the Department. The Vendor shall submit, Attachment "D", Certificate of Contract Completion with the final invoice.

- 4.9** In the event that funds paid to the Vendor under this contract are subsequently disallowed by the Department because of accounting error or charges not in conformity with this contract, the Vendor agrees that such disallowed amounts are due to the Department upon demand. Further, Vendor agrees that the Department shall have the right to deduct from any payment due to the Vendor under any other contract between the Vendor and the Department or under this contract, an amount sufficient to satisfy any amount due and owing the Department by the Vendor under this contract.

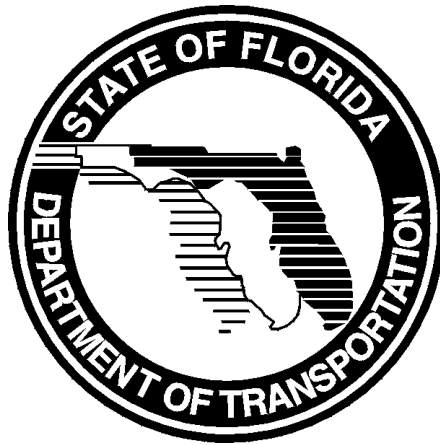


EXHIBIT "C"

PRICE PROPOSAL

RFP-DOT- 09/10-8001-KB

PAYMENT CARD INDUSTRY (PCI) SERVICES

FPI No. 423249-1-32-01

Exhibit "C"
Price Proposal
Payment Card Industry (PCI) Services

RFP-DOT-09/10-8001-KB
FPI No. 423249-1-32-01

First Year Prices						
PAY ITEM NO.	DESCRIPTION	UNIT	QTY. OF ITEM*	UNIT RATE PRINTED OUT IN LONGHAND	UNIT RATE	PAY ITEM TOTAL
Routine PCI Services						
1	All Payment Card Industry (PCI) Services Level 1 Merchant and Business Impact Analysis (BIA) Exhibit "A" Section 4.0 -4.6.5	Lump Sum	1	_____ Dollars and _____ Cents	\$ _____.____	\$ _____.____
Additional Services - First Year Prices						
PAY ITEM NO.	DESCRIPTION	UNIT	QTY. OF ITEM*	UNIT RATE PRINTED OUT IN LONGHAND	UNIT RATE	PAY ITEM TOTAL
2	PCI Audit Services (remediation consulting)	Per Hour	1	_____ Dollars and _____ Cents	\$ _____.____	\$ _____.____
3	Forensic Security Services Exhibit "A" section 4.5	Per Hour	1	_____ Dollars and _____ Cents	\$ _____.____	\$ _____.____

TOTAL - FIRST YEAR \$ _____.____

Name of Business: _____
(Please Print)

Exhibit "C"
Price Proposal
Payment Card Industry (PCI) Services

RFP-DOT-09/10-8001-KB
FPI No. 423249-1-32-01

Second Year Prices						
PAY ITEM NO.	DESCRIPTION	UNIT	QTY. OF ITEM*	UNIT RATE PRINTED OUT IN LONGHAND	UNIT RATE	PAY ITEM TOTAL
Routine PCI Services						
4	All Payment Card Industry (PCI) Services Level 1 Merchant and Business Impact Analysis (BIA) Exhibit "A" Section 4.0 -4.6.5	Monthly	12	_____ Dollars and _____ Cents	\$_____.____	\$_____.____
Additional Services - Second Year						
PAY ITEM NO.	DESCRIPTION	UNIT	QTY. OF ITEM*	UNIT RATE PRINTED OUT IN LONGHAND	UNIT RATE	PAY ITEM TOTAL
5	PCI Audit Services (remediation consulting)	Per Hour	1	_____ Dollars and _____ Cents	\$_____.____	\$_____.____
6	Forensic Security Services Exhibit "A" Section 4.5	Per Hour	1	_____ Dollars and _____ Cents	\$_____.____	\$_____.____

TOTAL - SECOND YEAR \$_____.

Name of Business: _____
(Please Print)

Exhibit "C"
Price Proposal
Payment Card Industry (PCI) Services

RFP-DOT-09/10-8001-KB
FPI No. 423249-1-32-01

Third Year Prices						
PAY ITEM NO.	DESCRIPTION	UNIT	QTY. OF ITEM*	UNIT RATE PRINTED OUT IN LONGHAND	UNIT RATE	PAY ITEM TOTAL
Routine PCI Services						
7	All Payment Card Industry (PCI) Services Level 1 Merchant and Business Impact Analysis (BIA) Exhibit "A" Section 4.0 -4.6.5	Monthly	12	_____ Dollars and _____ Cents	\$_____.____	\$_____.____
Additional Services - Third Year						
PAY ITEM NO.	DESCRIPTION	UNIT	QTY. OF ITEM*	UNIT RATE PRINTED OUT IN LONGHAND	UNIT RATE	PAY ITEM TOTAL
8	PCI Audit Services (remediation consulting)	Per Hour	1	_____ Dollars and _____ Cents	\$_____.____	\$_____.____
9	Forensic Security Services Exhibit "A" Section 4.5	Per Hour	1	_____ Dollars and _____ Cents	\$_____.____	\$_____.____

TOTAL - THIRD YEAR \$_____.

Name of Business: _____
(Please Print)

Exhibit "C"
Price Proposal
Payment Card Industry (PCI) Services

RFP-DOT-09/10-8001-KB
FPI No. 423249-1-32-01

First Year Renewal Prices (4th Contract Year)						
PAY ITEM NO.	DESCRIPTION	UNIT	QTY. OF ITEM*	UNIT RATE PRINTED OUT IN LONGHAND	UNIT RATE	PAY ITEM TOTAL
Routine PCI Services						
10	All Payment Card Industry (PCI) Services Level 1 Merchant and Business Impact Analysis (BIA) Exhibit "A" Section 4.0 -4.6.5	Lump Sum	1	_____ Dollars and _____ Cents	\$ _____.	\$ _____.
Additional Services - First Renewal Year Prices						
PAY ITEM NO.	DESCRIPTION	UNIT	QTY. OF ITEM*	UNIT RATE PRINTED OUT IN LONGHAND	UNIT RATE	PAY ITEM TOTAL
11	PCI Audit Services (remediation consulting)	Per Hour	1	_____ Dollars and _____ Cents	\$ _____.	\$ _____.
12	Forensic Security Services Exhibit "A" Section 4.5	Per Hour	1	_____ Dollars and _____ Cents	\$ _____.	\$ _____.

TOTAL - FIRST YEAR RENEWAL

\$ _____.

Name of Business: _____

Exhibit "C"
Price Proposal
Payment Card Industry (PCI) Services

RFP-DOT-09/10-8001-KB
FPI No. 423249-1-32-01

Second Year Renewal Prices (5th Contract Year)						
PAY ITEM NO.	DESCRIPTION	UNIT	QTY. OF ITEM*	UNIT RATE PRINTED OUT IN LONGHAND	UNIT RATE	PAY ITEM TOTAL
Routine PCI Services						
13	All Payment Card Industry (PCI) Services Level 1 Merchant and Business Impact Analysis (BIA) Exhibit "A" Section 4.0 -4.6.5	Monthly	12	_____ Dollars and _____ Cents	\$ _____.	\$ _____.
Additional Services - Second Year Renewal						
PAY ITEM NO.	DESCRIPTION	UNIT	QTY. OF ITEM*	UNIT RATE PRINTED OUT IN LONGHAND	UNIT RATE	PAY ITEM TOTAL
14	PCI Audit Services (remediation consulting)	Per Hour	1	_____ Dollars and _____ Cents	\$ _____.	\$ _____.
15	Forensic Security Services Exhibit "A" Section 4.5	Per Hour	1	_____ Dollars and _____ Cents	\$ _____.	\$ _____.

TOTAL - SECOND YEAR RENEWAL \$ _____.

Name of Business: _____
(Please Print)

Exhibit "C"
Price Proposal
Payment Card Industry (PCI) Services

RFP-DOT-09/10-8001-KB
FPI No. 423249-1-32-01

--

Third Year Renewal Prices (6th contract Year)						
PAY ITEM NO.	DESCRIPTION	UNIT	QTY. OF ITEM*	UNIT RATE PRINTED OUT IN LONGHAND	UNIT RATE	PAY ITEM TOTAL
Routine PCI Services						
16	All Payment Card Industry (PCI) Services Level 1 Merchant and Business Impact Analysis (BIA) Exhibit "A" Section 4.0 -4.6.5	Monthly	12	_____ Dollars and _____ Cents	\$ _____.	\$ _____.
Additional Services - Third Year Renewal						
PAY ITEM NO.	DESCRIPTION	UNIT	QTY. OF ITEM*	UNIT RATE PRINTED OUT IN LONGHAND	UNIT RATE	PAY ITEM TOTAL
17	PCI Audit Services (remediation consulting)	Per Hour	1	_____ Dollars and _____ Cents	\$ _____.	\$ _____.
18	Forensic Security Services Exhibit "A" Section 4.5	Per Hour	1	_____ Dollars and _____ Cents	\$ _____.	\$ _____.

TOTAL - THIRD YEAR RENEWAL

\$ _____.

Name of Business: _____
(Please Print)

Exhibit "C"
Price Proposal
Payment Card Industry (PCI) Services

RFP-DOT-09/10-8001-KB
FPI No. 423249-1-32-01

PAY ITEMS 1 -3 TOTAL YEAR 1: _____

PAY ITEMS 4 -6 TOTAL YEAR 2: _____

PAY ITEMS 7 -9 TOTAL YEAR 3: _____

PAY ITEMS 10 -12 TOTAL RENEWAL YEAR 1: _____

PAY ITEMS 13 -15 TOTAL RENEWAL YEAR 2: _____

PAY ITEMS 16 -18 TOTAL RENEWAL YEAR 3: _____

TOTAL : _____

Business Name: _____

EXHIBIT "C"
PRICE PROPOSAL
PAYMENT CARD INDUSTRY (PCI) SERVICES

The undersigned has completed and is returning the following documents as part of its Price Proposal Package and understands that failure to return any of these documents fully completed may cause rejection of the Proposal.

The following forms must be completed and submitted by the proposal due date and time, in order for the Proposal to be responsive:

___ Price Proposal: Exhibit C, Pages 1-8

___ All forms supplied with the advertisement package (Forms 1 through 4). Be certain to fill in all the blanks on the forms supplied; do not leave any blank lines on the forms.

Name of Business: (Print) _____ Federal I.D. No: _____

Mail Address _____ Certified MBE: yes ___ No ___

Street Address _____ Certified DBE: yes ___ No ___

City _____ County _____ State _____ Zip _____ - _____

Phone Number () _____ - _____ Fax No.() _____ - _____ Internet e-mail Address _____

Authorized Signature _____ Title _____
Name (Owner, President, or Designated Officer in Corp. Resolution)*

Print/Type Name Mr. ___ Ms. ___ Date _____, 200__

Emergency Contact Information: _____ Title _____

Phone No. () _____ - _____ Fax No.() _____ - _____ Beeper No. () _____ - _____

Emergency Contact Information: _____ Title _____

Phone No. () _____ - _____ Fax No.() _____ - _____ Beeper No. () _____ - _____

If signature is other than as listed, then the person signing for the firm, must be authorized to do so in the company Corporation Resolution. If this is the case then a copy of the Corporation Resolution shall be furnished along with the bid package.