SECOND AMENDMENT TO THE AGREEMENT FOR CONSULTING SERVICES BETWEEN THE CITY OF SAN JOSE AND VERISIGN, INC.

This Second Amendment to the Agreement for Information Security Consultant Services is entered into effective the _____ day of June 2009, by the City of San José ("City"), a municipal corporation, and VeriSign Inc., a Delaware corporation ("Consultant").

RECITALS

WHEREAS, on April 3, 2008, City and Consultant entered into an agreement entitled "AGREEMENT FOR CONSULTANT SERVICES TO PERFORM A SECURITY AUDIT BETWEEN THE CITY OF SAN JOSE AND VERISIGN, INC.", and

WHEREAS, on August 26, 2008, City and Consultant entered into a First Amendment to the Agreement to include additional services, and extend the term of the Agreement to June 30, 2009, and increase the total compensation to an amount not to exceed $349,760, and

WHEREAS, the City has determined that it has need for Consultant to perform additional services on the same project:

NOW THEREFORE, the parties agree to amend the Agreement as follows:

1. Section 1 of the Agreement is amended by adding services set forth in Exhibit G of this document which is attached hereto and incorporated herein.

2. Section 2 of the Agreement is amended to read as follows:

   The term of this Agreement shall be from April 3, 2008 to June 30, 2010, inclusive, subject to the provisions of Section 11 of this Agreement.

3. Section 4 of the Agreement is amended to read as follows:

   The compensation to be paid to Consultant, including both payment for professional services and reimbursable expenses shall not exceed Three Hundred Ninety Nine Thousand Seven Hundred Sixty Dollars ($399,760).

4. Exhibit B "Compensation" is amended to read as set forth in Revised Exhibit B that is attached here to and incorporated herein.

5. All of the terms and conditions of the original Agreement and First Amendment not modified by this Second Amendment shall remain in full force and effect.

APPROVED AS TO FORM:

_____
Brian Doyle
Senior Deputy City Attorney

City of San José
A municipal corporation

By:_____
Name: Deanna Santana
Title: Deputy City Manager

VeriSign, Inc.
A Delaware Corporation

By:_____
Name:
Title:

Revised Exhibit B
COMPENSATION

COMPENSATION SPECIFIC TO WORK PERFORMED UNDER THE ORIGINAL OR "BASE" AGREEMENT:

CITY agrees to compensate CONSULTANT at the fixed rate cost of $221,760 for professional services and no more than $28,000 for reimbursable expenses performed in accordance with the terms and conditions of this AGREEMENT. CONSULTANT shall provide City with an invoice for total cost at completion and City acceptance of all deliverables. Payment shall be made to CONSULTANT within fourteen (14) days of City's acceptance of all deliverables.

Project Deliverable 1: Preparation of Detailed Report - Prepare a detailed audit report that presents prioritized list of vulnerabilities identified and the key category of services that the vulnerability may effect (i.e. authentication, file/print, email, www, etc.). Define a risk level for each vulnerability such as the following format

- Critical
- Major
- Minor
- Informational
- Detailed list of possible solutions to each vulnerability
- Estimate implementation time and cost for recommended solutions
- Recommend skill sets required to implement solutions
- Identify potential impacts related to implementation of recommended solutions
- If distinctive needs for Police and Airport are identified, the City will determine if separate assessment reports should be submitted.

Project Deliverable 2: Benchmarking – The City is interested in determining how the current practices of the organization compares with those of industry and other public sector organization's best practices. Consultant will provide a detailed report with the following key information:

- Include names of organizations and types of systems compared
- Include size of staff focused on security
- Provide a direct comparison of the practices of the City vs. private industry or public sector organization

Project Deliverable 3: Citywide Security Governance Model – Security crosses many departmental boundaries, and the City has a distributed IT model. The City is interested in gaining a better understanding of how both central IT and the outlying departments are addressing security issues individually and collectively. The Consultant will provide a detailed report following interviews with key IT staff and/or Executive management from the following departments:

- Information Technology
- Police
- Airport
- Environmental Services

The report should include the following:

- Areas of overlap between departments and / or IT
- Areas of unique needs by departments
- Each department above ability to address its collective and unique security needs using staff, software, hardware, policies, practices, etc.
- A recommendation of areas in which the City can leverage its investment by pooling resources (staff, software, hardware, policies, practices, etc.)

Project Deliverable 4: Final Report, Recommendations and Direction – At the conclusion of this engagement, the consultant will make a presentation to the stakeholders of this project and at a closed session of the San José City Council. Key points from the assessment report and specific key issues and recommendations will also be presented. The Consultant will prepare and submit a final report at the time of presentation that includes each of the documents outlined in the prior tasks. These reports, along with the presentation, will serve as the final deliverable for this consulting agreement. The final report will be formatted in the following manner:

- Introduction to include a summary scope of work as described in the RFP entitled *Consultant Services for the Audit of Information Security* dated July 11, 2007.
- A summary of CONSULTANT's qualifications to meet the requirements set forth in the Scope of Services
- An executive overview of the findings and recommendations for the audit
- Benchmarking and security governance tasks
- A detailed section consisting of Project Deliverables 1-2 above
- An appendix section consisting of details in Project Deliverable 3 above.

REIMBURSABLE EXPENSES

CONSULTANT'S reimbursable expenses shall be based on actual out-of-pocket and travel related expenses (including transportation, hotels, meals, etc.) and will be billed at the end of the engagement, with the final project invoice for professional services. Total reimbursable expenses (travel and miscellaneous) shall not exceed Twenty Eight Thousand Dollars ($28,000) for work on the original agreement and First Amendment, and Five Thousand Dollars ($5,000) on this Second Amendment.

COMPENSATION SPECIFIC TO WORK PERFORMED UNDER AMENDMENT 1 TO THE AGREMENT:

City shall reimburse Contractor on a time and material basis for actual costs incurred at the following rates:

Work Description	Unit	Rate	Comments
Policy Work	Per hour	$225.00	
PCI Work	Per hour	$250.00	
Travel expenses		As incurred	Customary and reasonable
Other expenses		As incurred	Customary and reasonable

COMPENSATION SPECIFIC TO WORK PERFORMED UNDER AMENDMENT 2 TO THE AGREMENT:

City shall reimburse Contractor on a time and material basis for actual costs incurred at the following rates:

Work Description	Unit	Rate	Comments
Trusted Advisor	Per hour	$275.00	
Compliance Assessment	Per hour	$250.00 (QSA) $275.00 (Lead)	
Travel expenses		As incurred	Customary and reasonable
Other expenses		As incurred	Customary and reasonable

On-site work shall be billed at a minimum of four (4) hours per site visit.

Consultant shall invoice City monthly and City shall pay Contractor within thirty days after receipt of a properly completed invoice with the reference number AC20994. This contract will serve in lieu of a purchase order. The billing contact and address for all invoices is as follows:

Sharon Covarrubias
City of San José
Information Technology Dept.
200 E. Santa Clara Street, 11th Floor
San José, CA 95113

Consultant's invoice shall itemize all hours worked during invoice period by work description.

MAXIMUM COMPENSATION

The maximum amount of compensation to be paid to CONSULTANT under this AGREEMENT including both payment for professional services and reimbursable expenses, shall not exceed Three Hundred Ninety Nine Thousand Seven Hundred Sixty Dollars ($399,760) which includes Three Hundred Forty Nine Thousand Dollars ($349,000) on the original Agreement and First Amendment, and Fifty Thousand Dollars ($50,000) on this Second Amendment. Any hours worked for which payment would result in a total exceeding the maximum amount of compensation set forth herein shall be at no cost to CITY.

EXHIBIT G

CITY OF SAN JOSE (AIRPORT)
ON-SITE PCI DATA SECURITY STANDARD COMPLIANCE ASSESSMENT

STATEMENT OF WORK

Presented To:
Diane Mack-Williams
IT Director
Airport Technology Services
1732 N. First Street, Suite 600
San Jose, CA 95112-4538
Telephone: (408) 501-7755
Email:dmack-williams@sjc.org

Submitted By:
Richard Nadzam
Senior Territory Manager
VeriSign, Inc.
685 E. Middlefield Rd
Mountain View, CA 94043
Telephone: (650) 426-3264
Fax: (650) 237-8865
Email: RNadzam@verisign.com

May 27, 2009

Global Security Consulting

Table of Contents

Notice

VeriSign has made every reasonable attempt to ensure that the information contained within this statement of work is correct, current and properly sets forth the requirements as have been determined to date. The parties acknowledge and agree that the other party assumes no responsibility for errors that may be contained in or for misinterpretations that readers may infer from this document.

Non-Disclosure Statement

The information in this document is VeriSign Confidential, and cannot be reproduced or redistributed in any way, shape, or form without prior written consent from VeriSign, Inc.

Trademark & Copyright Notice

1.0 General Information

This Statement of Work ("SOW"), effective as of the date of the last signature on the signature page to this Statement of Work ("Effective Date"), is by and between VeriSign, Inc., together with its wholly owned subsidiaries ("VeriSign") and City of San Jose ("CSJ", "Customer"). The parties hereby agree as follows:

This Statement of Work is governed by the terms and conditions set forth in the Agreement for Information Security Consultant Services, executed between the parties on the 26th day of August, 2008 by the City of San Jose ("City") and VeriSign, Inc. and any other terms and conditions set forth in Section 1.1 of this SOW. The information in this document is VeriSign Confidential, and cannot be reproduced or redistributed in any way, shape, or form without prior written consent from VeriSign, Inc.

For the avoidance of doubt, Customer hereby acknowledges and agrees that the offer of pricing and other terms set forth in this Statement of Work shall be valid for 45 days after the date set forth on the cover sheet of this Statement of Work. The offer of pricing and other terms set forth in this Statement of Work shall become effective and binding on VeriSign and Customer only upon the execution of this Statement of Work by the parties on the Effective Date.

1.1 Background & Objectives

This SOW presents VeriSign's methodology, pursuant to which VeriSign, as a Qualified Security Assessor ("QSA") for PCI Security Standards Council LLC ("PCICo"), will perform an on-site assessment (the "Compliance Assessment") of Customer to determine Customer's compliance with the Payment Card Industry Data Security Standard, as may be amended from time to time, and the contemporaneous version of which is available for review on the PCICo Web site at http://www.pcisecuritystandards.org (the "PCI Standard").

VeriSign understands that Customer is considered a network managed services entity performing services for a member financial institution of Member ("Member" means a then current member of PCICo). As such, the PCI Standard requires a Compliance Assessment. This Compliance Assessment will specifically target CSJ's areas where they impact cardholder security on the behalf of their merchants.

During the assessment, VeriSign will assess CSJ's compliance with the requirements established by the PCI Standard. For areas that are found out of compliance with the requirements, VeriSign will make recommendations to bring CSJ into compliance and strengthen its overall security program. Remediation of non-compliant areas is not included herein, but may be covered in a separate SOW if so desired.

This SOW includes:

- Scope of Work – VeriSign's methodology for conducting the Compliance Assessments and our analysis of how the various requirements of the Compliance Assessment intersect.
- Deliverables – Description of the deliverables for this project.
- Pricing – VeriSign's pricing model for this engagement and the included components.
- Project Assumptions – any assumptions that were used to derive the scope of work or pricing for this engagement.

This SOW does not cover the cost of quarterly vulnerability scans or other ongoing requirements covered in the PCI Standard. VeriSign can provide a separate SOW for any of these activities if desired.

CSJ acknowledges and agrees that, notwithstanding the confidentiality obligations of CSJ and VeriSign in connection with this SOW in the Master Services Agreement, VeriSign may from time to time, as required pursuant to VeriSign's contractual obligations to PCICo, disclose the Report on Compliance related to the CSJ and any other related information (including Compliance Assessment results set forth in Section 5.1) to PCICo and/or its Members and each Member may disclose such information on an as needed basis to such Member's financial institutions and issuers and to relevant governmental, regulatory and law enforcement inspectors, regulators and agencies, and that such Member has received a Report on Compliance and other related information with respect to the CSJ and whether the Report on Compliance is satisfactory. CSJ further acknowledges and agrees that VeriSign is obligated to provide PCICo and its Members with such available reviews and reports to monitor VeriSign's compliance as a QSA. In connection therewith, CSJ agrees to make available such reviews and reports that PCICo and/or a Member may request from time to time.

1.2 Key Business and Technical Contacts

1.2.1 City of San Jose Business Contact Information

Name:	Diane Mack-Williams IT Director
Mailing Address:	Airport Technology Services 1732 N. First Street, Suite 600 San Jose, CA 95112-4538
E-Mail Address:	dmack-williams@sjc.org
Phone Number:	(408) 501-7755

1.2.2 VeriSign Business Contact Information

Name:	Richard Nadzam Senior Territory Manager
Mailing Address:	VeriSign, Inc. 685 E. Middlefield Road Mountain View, CA 94043
E-Mail Address:	rnadzam@verisign.com
Phone Number:	(650) 426-3264
Fax Number:	(650) 237-8865

1.2.3 VeriSign Technical Contact Information

Name:	Steve Levinson Senior Consulting Manager
Mailing Address:	VeriSign, Inc. 2242 Via Tiempo Cardiff, CA 92007
E-Mail Address:	slevinson@verisign.com
Phone Number:	(619) 241-3287

2.0 SERVICE DESCRIPTION

This section provides a description of services, scope of activity, and required support requirements associated with the services.

2.1 General Description

The PCI Data Security Standard defines the scope of the assessment as the infrastructure, policies, and practices that are directly related to authorization and settlement of Member branded card ("Payment Card") transactions. The table in Section 2.2, which is based on conversations with CSJ's staff, presents the scope of the Compliance Assessment of this SOW. The PCI Standard allows for sampling of the infrastructure. Since there are no Internet-facing devices in scope in this case, no external perimeter scan is required. VeriSign will review CSJ for compliance to the 1.2 version of the PCI Data Security Standard.

The tasks listed below are designed to fulfill the annual Compliance Assessment which is to be performed by an authorized third party. In order to achieve full compliance, CSJ must also complete an annual penetration test. The scope of these engagements must include both networks and applications. VeriSign offers penetration testing services; however, they are not included within this SOW.

2.2 Scope of Activity

The scope outlined in Table 1: Project Scope is a representative sample of the infrastructure CSJ uses to process Payment Card transactions with the exception of the external perimeter assessment which includes the entire external footprint.

Table 1: Project Scope

Project Task	Comments
Configuration Reviews of Firewalls, Routers, and Switches	Up to 10 network devices Focused on security-related rule sets, not overall configuration
Interviews	Interviews of up to 20 persons
On-Site Locations	Number of office locations – 3 Number of data center locations – 3 Number of airport locations – 2 (includes San Jose Airport and parking enterprise)
Documentation Review	VeriSign will review pertinent documentation as part of the engagement. The documentation reviewed in a typical assessment is listed in Section 3.2.1

2.3 Trusted Advisor

VeriSign is a respected industry leader in all of the PCI approved assessor categories. We have one of the largest concentrations of QSAs and QPASPs in the US, as well as presence in EMEA, CALA, and the Pacific Rim. Our high volume of top Level 1

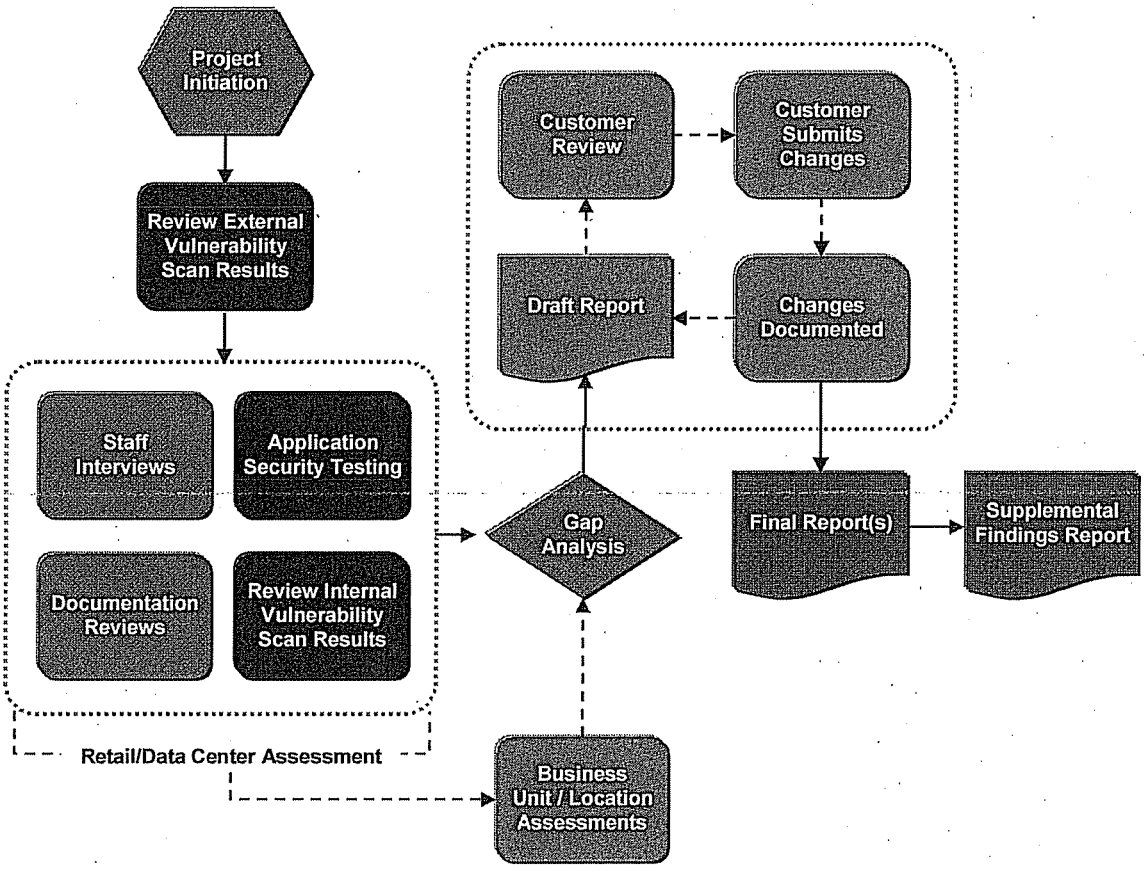
companies provides us an extensive mind share of the Data Security Standard, experience in precedence-based compensating controls, and an unrivaled relationship with the card brands and PCI Co. CSJ will purchase a block of twenty consulting hours that will be consumed on a Time & Expense basis for PCI compliance expertise and guidance. VeriSign approaches the details of each PCI project uniquely to the customer; however, our general approach for CSJ is as follows:

- Provide feedback pertaining to CSJ's strategies, architecture, and systems from both a PCI QSA perspective as well as from a security industry Best Practices perspective.
- VeriSign will consult with each group to understand their function and contribution to the payment process.
- VeriSign will work closely with CSJ to help create a PCI strategy for the airport parking enterprise.
- Develop documentation needed for PCI compliance. VeriSign will create documentation when CSJ makes a request to create needed documents for PCI compliance.
- VeriSign will provide CSJ with periodic updates on PCI industry trends and risks domestically and internationally.

3.0 APPROACH AND METHODOLOGY

This section presents VeriSign's approach to conducting the Compliance Assessment. It includes project initiation, assessment approach, and any remediation follow-up. Each of these project phases is clearly defined below. At the conclusion of this project, CSJ will be provided a Report on Compliance ("ROC") which will clearly identify any findings and recommendations to assist CSJ in reaching compliance with the PCI Standard. It is important to note that VeriSign does not offer any opinions of legal compliance. The following figure provides a visual sample of VeriSign's assessment process.

Figure 1: PCI Assessment Flow



3.1 Project Initiation

Upon commencement of our service to CSJ, VeriSign will conduct a kick-off meeting (phone conference, or in person) to establish rules of engagement and share critical information.

The kickoff meeting will accomplish the following tasks:

- Perform introductions with key people at CSJ and VeriSign
- Explain VeriSign's role to CSJ
- Review the scope of services for this engagement
- Review communication, notification, and issue escalation procedures
- Discuss the frequency and method of communication for regular status meetings
- Review CSJ's network topology
- Review critical applications that process Payment Card data
- Discuss other CSJ specific requests and rules of engagement
- Discuss scoping for sampling of connected systems
- Discuss the involvement of CSJ's technical staff in the project for the purpose of knowledge transfer and security
- Arrange methods for secure document sharing, status reporting, and vulnerability escalation
- Establishment of primary and secondary contact persons at CSJ and VeriSign, and exchange contact information including secure email methods
- Discuss the documentation or deliverables required at completion of the project

VeriSign's approach is highly collaborative. At any point during the Compliance Assessment, an identified non-compliant issue will be communicated to the Points of Contact in a manner agreed upon during this kickoff meeting.

3.2 PCI Standard Assessment Methodology

This section presents VeriSign's approach to conducting the Compliance Assessment for CSJ. It includes our assessment approach and remediation follow-up. VeriSign will conduct a full review to the level of detail required to report CSJ's compliance with the PCI Standard. All twelve control areas of the PCI Standard will be covered and a ROC in the required format will be generated for CSJ.

The 12 control areas are as follows:

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 or programs
- 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 for employees and contractors

3.2.1 Documentation Review

To conduct the high-level policy and process review, VeriSign will use knowledge of the PCI Standard to review the policy program, device rule sets, and processes CSJ employs to ensure information security.

The following is an example of documents that VeriSign will review in a typical assessment:

- Acceptable Use
- Business continuity planning
- Asset classification and control
- Change control process

- Computer and system management
- Configuration and hardening standards (servers, firewalls, network devices, databases)
- Data flow diagrams (cardholder data)
- Data retention and handling
- Firewall and network administration policy
- Firewall rule sets
- HR hiring and training practices
- Incident Response Plan
- Information Security Policy
- Legal contracts with third parties that handle Payment Card data
- Network diagrams
- Patching policy
- Personnel security
- Physical and environmental security
- Router/switch configurations
- System access controls
- System development and maintenance
- Security daily operational procedures
- Security organization
- Wireless policy (if applicable)

3.2.2 Personnel Interviews

To assess the implementation of the policies, VeriSign will conduct a number of process interviews with various personnel at CSJ. Following is a sample list of functional groups from which VeriSign would need to interview personnel.

This list will be modified to reflect the business model CSJ employs:

- Network Administration
- Information Security including the CSO or CISO
- Security Administration
- Database Administration
- Human Resources
- Application Development
- Business Units that may have contact with Payment Card information
- Legal

3.3 Follow-up Validation

Should non-compliant issues be identified that CSJ prefers to correct without VeriSign's assistance or if these issues cannot be corrected during the time frame of the Compliance Assessment, VeriSign will return to CSJ once remediation is complete to validate their compliance on a "time and expense" basis. This effort will be addressed with a separate SOW, if required.

3.4 Compliance Recommendations

VeriSign's approach is highly collaborative. Upon discovery of a non-compliant area, VeriSign will immediately inform CSJ. Thereafter, VeriSign will review with CSJ various options to meet compliance.

CSJ may not meet a requirement as specified in the PCI Standard in some cases, but still have sufficient compensating controls to meet the intent and rigor as required by the standard. In these instances, VeriSign will obtain more detailed information in order to adequately convey the method and level of security CSJ achieves with the current method. VeriSign will make a determination as to whether the controls achieve the level of risk mitigation established by the PCI Standard and comment appropriately. Based on VeriSign's close relationship with the Payment Card Industry, we are often able to provide an initial assessment of the acceptability of the approach. To date, VeriSign has not had a compensating control determination rejected.

In cases where there are no compensating controls or mitigation methods, VeriSign will make recommendations that will provide CSJ direction for achieving compliance with the specific requirement.

4.0 SCHEDULE

4.1 Period of Performance

CSJ requests the following project dates. VeriSign will make every reasonable attempt to meet the dates requested. CSJ understands and agrees that changes in critical factors (such as those listed below in Project Change Control, or a delay in execution of this document) may impact VeriSign's ability to meet certain dates.

Project Start Date:	Within two (2) weeks of Effective Date
Project Completion Date:	December 31, 2009

4.2 Project Change Control

VeriSign has made every attempt to accurately estimate time required to successfully complete the project. CSJ acknowledges and agrees that if impediments, complications, or CSJ requested changes in scope arise, these factors are out of the control of VeriSign, and the length of the project and associated price could be impacted. Examples of valid impediments, complications, and changes in scope consist of (but are not limited to):

- CSJ initiated delay where Customer is not prepared to allow VeriSign to begin work on the agreed upon start date thus resulting in additional cost to VeriSign for resources that have been sent to CSJ's site but can not begin the Services.
- CSJ provided information necessary for timely delivery by VeriSign is not accurate.
- Delays or problems associated with third party telecommunication equipment. (This includes, but is not limited to, cabling, servers, routers, hubs, and switches managed or installed by third parties.)
- Malfunctioning hardware.
- Inability to access equipment or personnel that are required to complete the project.
- Conflicts or incompatibilities associated with the installation of hardware or software installed by VeriSign.
- CSJ increases the scope of services requiring additional labor, hardware, software, materials, travel, lodging, meals, or other direct costs.

If any change(s) from impediments, complications, or CSJ changes in the scope of services cause an increase or decrease in the price or level of effort of the SOW, or the time required for the performance of any part of the work to be accomplished hereunder, whether or not such work is specifically identified in the written change, then the price, delivery schedules and other affected provision(s), if any, as applicable, shall be equitably adjusted and this SOW shall be modified in writing by the mutual agreement of the parties in accordance with this Section.

5.0 SERVICE DELIVERABLES

5.1 Description

VeriSign will provide the following deliverables as part of this project:

Name of Deliverable	Description of Deliverable
PCI DSS Remediation Roadmap	This report is provided to CSJ at the conclusion of the PCI assessment. The purpose of this report is to outline high-level findings (gaps) and to present a strategic plan to address these gaps.
PCI DSS Report on Compliance	This report is provided to CSJ to satisfy the PCI reporting requirements. The format of this document is defined in PCI DSS Security Audit Procedures and Reporting (available at http://pcisecuritystandards.org/). VeriSign will submit a copy of the final Report on Compliance to PCICo and its Members, in accordance with Section 1.1 of this SOW to comply with VeriSign's reporting requirements to PCICo. A sample of this report is provided in Error! Reference source not found..
Attestation of Compliance ("AoC")	Provided CSJ achieves a fully compliant Report on Compliance, VeriSign will produce a signed Attestation of Compliance as required to prove compliance.
Supplemental Findings Report	This report is a supplement to the Report on Compliance and contains items that are not material enough to be included into the ROC itself, such as Suggested Practices suggestions or opportunities to improve security posture.

5.2 PCI DSS Remediation Roadmap

This report will outline high-level findings and present a strategic plan to address any gaps that would prevent CSJ from becoming PCI-compliant. The report will provide an overview of CSJ's PCI security posture along with a strategic plan that outlines and prioritizes remediation projects to convey an overall approach to achieving PCI compliance. This report shall include documentation of networks, systems, processes, and cardholder data flows subject to PCI DSS Standard.

5.3 PCI Standard Report on Compliance

The PCI Standard specifies the Reports on Compliance format that must be used for submission. VeriSign's report conforms to these requirements. The report format is provided below:

1. **Contact Information and Report Date**
   - Include contact information for the merchant or service provider, and assessor
   - Date of report
2. **Executive Summary**
   - Business description and how cardholder data is used

- List service providers, and other entities with whom the company shares cardholder data
- List processor relationships
- Whether entity is directly connected to a payment card company
- For merchants, POS products used
- Description of the sampling methodology for entities (stores, facilities) and system components including total population, number sampled, and rationale for number selected
- If applicable, description of how network segmentation reduced scope
- Any wholly-owned entities that require compliance with the PCI Standard
- Any international entities that require compliance with the PCI Standard
- Any wireless LANs and/or wireless POS terminals connected to the cardholder environment

3. **Description of Scope of Work and Approach Taken**
   - Version of the Security Audit Procedures document used to conduct the Compliance Assessment
   - Timeframe of assessment
   - Environment on which the Compliance Assessment was focused (i.e., client's Internet access points, internal corporate network, processing points for the payment card company, etc.)
   - Any areas excluded from the review
   - Brief description or high-level drawing of network topology and controls
   - Cardholder data flow diagram(s)
   - List of those interviewed
   - List of documentation reviewed
   - List of hardware and critical (e.g., database or encryption) software in use
   - Vulnerability scan results
   - For Managed Service Provider ("MSP") reviews, delineate which requirements apply to the MSP (and are included in the review), and which are not included in the review and are the responsibility of CSJ to review
4. **Findings and Observations**
   - Detailed findings matrix with in-depth discussion of the testing procedures and the results of the assessment
   - Where applicable, compensating controls will also be documented

5.4 Attestation of Compliance ("AoC")

In order to prove compliance to the PCI DSS, CSJ is required to produce an AoC that is signed by a QSA with the appropriate fields marked. VeriSign will use the approved template to customize one for CSJ provided they receive a fully compliant ROC under this SOW.

5.5 Supplemental Findings Report

PCI assessments are conducted in accordance with the current version of the Payment Card Industry Data Security Standard. The testing procedures within this standard require the Qualified Security Assessor obtain reasonable assurance the client has implemented the proper security controls surrounding the payment authorization and settlement process.

During the course of an assessment the QSA may observe projects, practices, or processes that may have an opportunity for improvement. Issues that fall into this category and are not material enough to be incorporated into the ROC are documented in this Supplemental Findings Report. This report contains a list of areas of improvement as well as a list of recommendations from VeriSign on remediation possibilities.

6.0 ASSUMPTIONS

VeriSign used the following assumptions during development of this SOW. Any changes to these assumptions may affect the price and schedule commitments.

- VeriSign is required to maintain a copy of all case logs, audit results, work papers, notes, and any technical information that was created and/or obtained during this assessment for a period of three (3) years per the Payment Card Industry (PCI) Data Security Standard Validation Requirements for Qualified Security Assessors, Section 4.6. If CSJ does not wish for VeriSign to maintain this documentation, CSJ will arrange a third party escrow service that both companies will have access to at CSJ's expense.
- CSJ will provide VeriSign access to the business, customer, and technical information, and facilities necessary to execute the solution.
- CSJ will provide VeriSign on-site and off-site access to documents necessary for this assessment.
- CSJ will ensure that appropriate personnel are available to meet with VeriSign, as necessary.
- The VeriSign professional working day is eight hours, including reasonable time for meals. VeriSign understands that occasions arise during customer engagements that require a longer or shorter working day. VeriSign will not be obligated to extend engagements when delays result from CSJ's inability to meet stated prerequisites prior to an engagement, nor when delays result from CSJ personnel not being available to provide required support.
- During this effort, VeriSign will not be responsible for negotiations with hardware, software, or other vendors, or any other contractual relationship between CSJ and third parties. VeriSign, at the request of CSJ, will provide input to CSJ regarding optimal product or vendor selection.
- Any application code, documentation, and/or presentations developed under this SOW will be in English.
- VeriSign will perform the work between 8:30am and 5:00pm (local time). After-hour and weekend work (when required), must be explicitly identified below or as otherwise agreed to in writing by the parties:

After-hours required?	Yes ☐	No ☒
Weekend hours required?	Yes ☐	No ☒
Location of onsite services?	CSJ 2000 E. Santa Clara St. - 11th Fl. San Jose, CA 95113 San Jose International Airport	

7.0 DISCLAIMER OF WARRANTIES

FURTHERMORE, EXCEPT AS SPECIFICALLY SET FORTH IN THIS STATEMENT OF WORK, THE SERVICES PERFORMED AND ANY ITEMS FURNISHED UNDER THIS STATEMENT OF WORK, INCLUDING BUT NOT LIMITED TO DATA, REPORTS, DOCUMENTATION, DELIVERABLES, HARDWARE AND SOFTWARE OF ANY KIND, AND ANY RECOMMENDATIONS OR CONCLUSIONS CONTAINED THEREIN, ARE PROVIDED ON AN "AS IS" BASIS WITH NO WARRANTIES OR REPRESENTATIONS OF ANY KIND. VERISIGN MAKES NO WARRANTY, EXPRESS OR IMPLIED, THAT ALL SECURITY THREATS AND VULNERABILITIES WILL BE DETECTED OR THAT THE SERVICES THEMSELVES OR COMPLIANCE WITH THE PCI STANDARD WILL RENDER CUSTOMER'S NETWORK AND SYSTEMS SAFE FROM MALICIOUS CODE, INTRUSIONS, OR OTHER SECURITY BREACHES.