Trustwave

Information Security & Compliance

Addendum

to the Compliance Validation Service Agreement dated September 30, 2005 &
MSA dated June 30, 2009

Presented To:

South Carolina Department of Revenue

Prepared By:

Carol Reif
Creif@trustwave.com
312.873.7272

ADDENDUM

This is an Addendum, dated as of the date executed below, to and governed by the Compliance Validation Services Agreement ("Agreement"), by and between Trustwave Holdings, Inc. ("Trustwave") and South Carolina Department of Revenue ("Client"), dated September 30, 2005. The Managed Security Services (IPS) shall be governed by the Master Services Agreement (MSA) dated June 30, 2009. TRUSTWAVE desires to provide additional Services, as identified below to Client, and Client wishes to receive such services pursuant to the terms and conditions, unless otherwise noted below, of the Agreement.

Purpose and Start Date

The purpose of this Addendum is to renew the services listed below and add any additional services, if they are selected. The services under this Addendum shall commence as of July 1, 2010.

Statement of Work

Compliance Validation Service (CVS)

Trustwave will provide South Carolina Department of Revenue with the CVS designed to manage the overall compliance process and aid in achieving the compliance objectives.

Trustwave QSAs and trained security experts will also support South Carolina Department of Revenue throughout the CVS process, to support internal efforts to gain compliance. This includes:

- ❑ **Remediation Guidance:** A Trustwave consultant will host weekly calls throughout a 4 week period after the initial questionnaire and scan are completed. The purpose of the calls will be to identify areas of non-compliance uncovered in the questionnaire and scan results, develop and assist in managing a remediation plan to address the non-compliance issues, validate policies and procedures, and review network security infrastructure and architecture.
- ❑ **Remote Support**: Throughout the project, Trustwave will provide comprehensive online support through the TrustKeeper portal that includes self-help and a continuously updated FAQ database. In addition, e-mail and multilingual phone support will be available during standard business hours to answer any questions regarding PCI DSS compliance or vulnerability scanning results.

To ensure comprehensive and efficient service, South Carolina Department of Revenue must fulfill its obligations within each item below before progressing to subsequent phases. Failure to do so may require an addendum to this contract that will include additional charges for any time or materials above and beyond those agreed to in this contract. The CVS does not include remediation services. If South Carolina Department of Revenue wishes to receive any remediation services, South Carolina Department of Revenue must specifically select those services.

Project Phases and Chronology

1. **<u>Phase I:</u> Online Questionnaire**

   PCI DSS requires that all merchants and service providers complete the PCI DSS self-assessment questionnaire. The TrustKeeper system provides an easy-to-use portal that satisfies the requirements of all the card associations with self-help and a continuously updated FAQ database. The questionnaire is available in English (American and British), French, Canadian French, Swedish, Greek, Spanish, Japanese and Chinese (Simplified and Traditional).

2. **<u>Phase II:</u> Vulnerability Scanning Service**

   Trustwave's proprietary managed external and internal scanning services enable an organization to meet its PCI requirements, while providing security, support, self-scan and reporting capabilities. PCI requirement 11.2 states that companies must run external and internal network scans at least quarterly and after any significant change in the network. To assist South Carolina Department of Revenue in meeting this requirement, Trustwave's CVS service will include:

External Vulnerability Scanning Service

The automated vulnerability scanning engine within TrustKeeper is a proprietary "intelligent" scanning solution that has been tested and determined to be compliant with the PCI Approved Scan Vendor (ASV) requirements. The scanning solution tests for more than 3,000 unique vulnerabilities and is extremely accurate in eliminating false positives. South Carolina Department of Revenue is entitled to receive monthly scans during the term of the Agreement for up to (**10**) IP addresses.

Trustwave's vulnerability scanning service provides South Carolina Department of Revenue with:

- □ **Reporting:** Through a secure web interface, TrustKeeper provides easy access to concise, auto-generated reports with a high-level summary for executives and managers. The reports also provide detailed results and remediation action for technicians. Remediation instructions include CVE-linked vulnerability checks and best practices defined by Trustwave consultants.
- □ **Security:** Trustwave's TrustKeeper infrastructure is monitored on a 24x7 basis to ensure protection of South Carolina Department of Revenue data. All South Carolina Department of Revenue data is delivered via secure channels.
- □ **Self-Service Scan Management:** Through the TrustKeeper secure web portal, with Trustwave's assistance, South Carolina Department of Revenue can define multiple scan profiles. South Carolina Department of Revenue can directly exclude specific IP addresses and ranges of IP addresses from scans. Blackout periods during which scans will not be conducted can be defined as well. Scans can be scheduled at a time that is convenient to South Carolina Department of Revenue's business operations, such as after the installation of new hardware or software. Scans can be run on an ad hoc or periodic basis.
- □ **Self-Service Scan Control:** From the TrustKeeper secure web portal, South Carolina Department of Revenue can easily start, stop and pause scans.
- □ **Remediation Management:** The TrustKeeper portal also provides tools for managing vulnerabilities. This allows for review of findings such as false positives, as well as assignment and tracking of remediation activities. The Remediation Management Report tracks the owner, status, target, and completion dates for each vulnerability.
- □ **E-mail Notification:** South Carolina Department of Revenue receives e-mail notifications before and after any scanning activity.
- □ **Support Services:** South Carolina Department of Revenue gains access to Trustwave's 24x7x365 Security Operations Center for assistance with general questions, and activities including establishing scan profiles and to exclude specific network ports from scanning on an individual target device or IP address range basis.

Trusted Commerce^{SM} Security Seal

With the Compliance Validation Service, South Carolina Department of Revenue receives the Trusted Commerce seal. Displaying the Trusted Commerce seal on the South Carolina Department of Revenue website will raise recognition of South Carolina Department of Revenue's commitment to payment card security and distinguish the organization as one that is committed to handling payment card data in a secure manner. The seal confirms South Carolina Department of Revenue's enrollment in Trustwave's program to validate compliance with the PCI DSS.

Once compliance has been achieved, customers that click on the Trusted Commerce seal will view a certificate stating that South Carolina Department of Revenue has completed the required actions for validation of PCI DSS compliance. The seal informs customers that, as a QSA, Trustwave examined South Carolina Department of Revenue's policies, procedures and technical systems and scanned South Carolina Department of Revenue payment card environment for vulnerabilities. This statement reassures customers that South Carolina Department of Revenue protects its payment card information as required by the PCI DSS, as well as reinforces customer trust.

Network Penetration Tests

The PCI DSS requirement 11.3 states that penetration testing must be performed against both external and internal environments within scope for the assessment on an annual basis. Trustwave's renowned security experts follow a proven methodology as they perform these security assessments. The steps of this methodology include:

1. **Network Mapping:** In the process of moving from general to specific, building an accurate network map of the externally facing devices is a critical task at the beginning of the penetration test. To support this, SpiderLabs will often need to obtain the network blocks from South Carolina Department of Revenue. This is typically in the form of a block of Internet addresses provided by one or many Internet Service Providers (ISPs). These addresses are then probed to see if they are in use (not for vulnerabilities at this time). The probes are executed three (3) times at different intervals during the first part of the engagement to ensure that no system is missed. The data gathered is used to create a network map of the external environment.
2. **System Identification and Classification:** The network map would not be very useful if the systems located on the network were not identified and classified. Another probe is performed of the systems identified, this time using TCP/IP and UDP/IP fingerprinting, service fingerprinting and various methods to identify and classify systems and services. The data gathered is used to classify the systems by function. Data gathered about the system helps to determine the classification. For example, a system running a particular version of the Apache Web Server as well as BEA Web Logic is most likely a web application server. After each system is classified the network map is updated to reflect each system's functionality and operation system. Before the next testing steps begin, SpiderLabs will debrief the South Carolina Department of Revenue key security contacts on specific system findings and intended target list to be used in the attack phase.
3. **System Vulnerability Identification:** All systems in the target network segment are probed, singularly and in tandem with the other hosts to locate potential vulnerabilities. Using a large working knowledge of exploit techniques, public information, and results of private vulnerability research, the Trustwave security consultants catalog all the potential attack vectors that might be exploitable. Trustwave security consultants devise several attack strategies and commence exploitation.
4. **System Vulnerability Exploitation:** If the plan of attack devised in the previous step includes any techniques that may impact production systems and infrastructure, South Carolina Department of Revenue is first advised of the possible system downtime that may arise. At this point it is up to South Carolina Department of Revenue to decide whether or not to proceed with the exploitation. As a rule, any potential vulnerability found is manually investigated, researched, and an attempt is made to exploit. Exceptions to this rule are techniques that will cause a denial of service (DoS) or harm the data on the target system. SpiderLabs will only attempt to exploit a DoS, or alter data on a target if specifically instructed by South Carolina Department of Revenue in writing. In exploiting vulnerability, SpiderLabs will make an attempt to either gain unauthorized access to the target system, or extract sensitive data from it. An exploit is considered successful if SpiderLabs is able to achieve either of these objectives. If successful exploitation leads SpiderLabs to systems compromise, SpiderLabs consultants will report the breach to the South Carolina Department of Revenue's key security personnel immediately.
5. **Application Architecture Identification:** Using the classifications previously established Trustwave will use tools and manual intervention to identify whether there are specific applications running on dynamic content servers within the target network. When an application server is identified, other systems will be identified within an application server group. This grouping will help identify potential flaws in application trust relationships. This information is vital to the successful identification of application vulnerabilities. In addition to identifying purposeful applications, Trustwave will attempt to discover backdoors that may be present in the environment.
6. **Application Exploitation:** Application exploitation is carried out on the public areas of exposed applications only, such as login fields, search functions or other publicly accessible areas. For applications that have public user registration functions, Trustwave WILL NOT attempt to create a

user to test authenticated areas of the application. Further, Trustwave WILL NOT perform a full Application Penetration Test against any application as part of an External Penetration Test. Trustwave will debrief South Carolina Department of Revenue's key security contacts on the applications identified, and what will be tested. If the system is a production system, South Carolina Department of Revenue will be advised of the possible system downtime that may arise. Each application will be tested with many different types of application penetration testing techniques related to input validation, business logic, application logic, session management and login routines.

7. **Compromise:** As systems or applications are compromised, South Carolina Department of Revenue's key security contacts will be notified. At that time, South Carolina Department of Revenue contacts will be given the opportunity to decide if the particular system should undergo additional tests. If it is decided to have Trustwave continue, additional techniques will be used to further penetrate the target system and the environment as a whole. This can include installation of network sniffers, remote management tools, connectivity tools, etc. Successful execution establishes a launch point for additional attacks against the environment.

8. **Data Extraction:** Each system that is compromised will be examined for the existence of critical data and files. If SpiderLabs finds such data to be accessible, a sample of this data will be downloaded from the system and securely stored by SpiderLabs until the presentation of deliverables.

9. **Further Compromise:** Once a system has been compromised, there are many trust relationships that can be potentially exploited. Data exposed through a compromise also might lead to the compromise of additional systems and applications. Using both data gathered and techniques similar to those used to develop the network map and system classification, SpiderLabs will launch a new stage of discovery against the environment.

[redacted]

[redacted]
[redacted]

[redacted]

[redacted]	[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

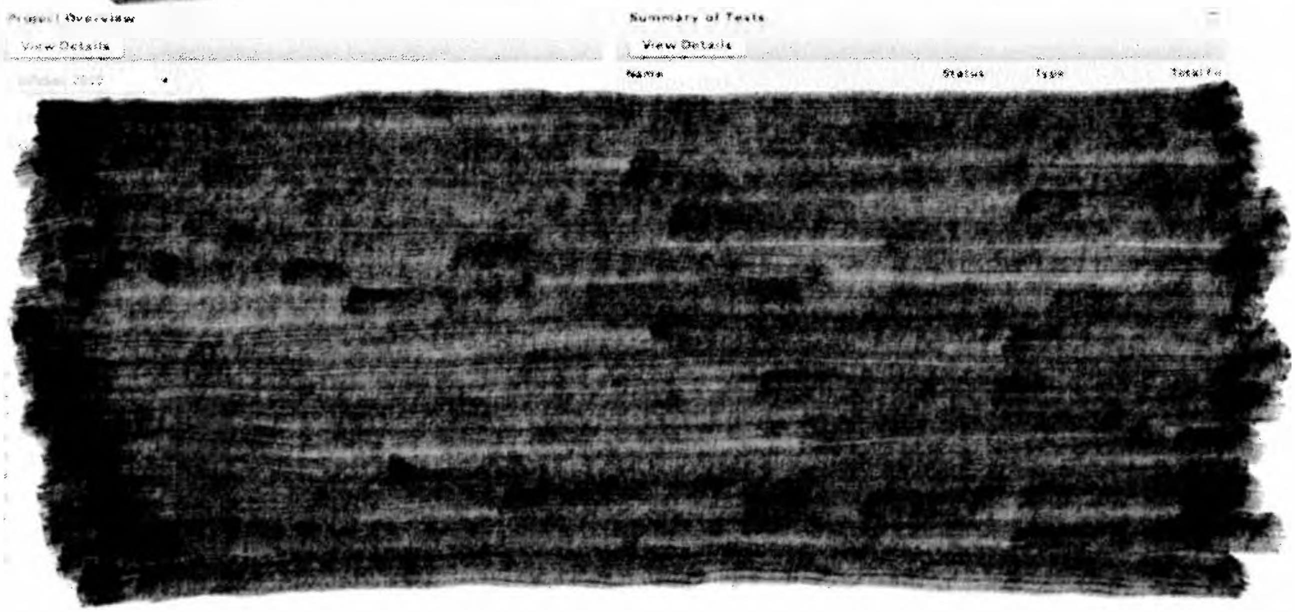
[redacted]

[redacted]

[redacted]

[redacted]

- ❑ [redacted]
- ❑ [redacted]
- ❑ [redacted]
- ❑ [redacted]
- ❑ [redacted]



[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

PRICING

Detailed Pricing Schedule

Trustwave Service	1-Year Term	3-Year Term	5-Year Term
Compliance Validation Service Package Includes • **Remote Validation and SAQ Assistance** • **External Vulnerability Scanning** • TrustKeeper account includes SAQ and external scanning for up to 512 IPs • PCI DSS reporting • **External Network Penetration Service** • **Internal Network Penetration Service**	$24,150	$20,800/yr.	$19,320/yr.
Managed Intrusion Prevention System (IPS) Service (TS-100)	$20,400	$18,000/yr.	$15,000/yr.
DLP Discover • Admin License includes unlimited scanning of servers, file shares, and PCs	$4,999	$4,500/yr.	$3,999/yr.
Total (if all services selected)	**$49,549**	**$43,300/yr.**	**$38,319/yr.**

***The services under this Addendum shall begin on July 1, 2011 for 1 year**
If client selects the 3 or 5 year term, the services shall automatically renew each year at the discounted rate indicated above as long as the Master Agreement remains active.

1. All services selected must be for the identical term.
2. Travel and expenses are not included in the fees and will be billed separately. Trustwave will use commercially reasonable efforts to travel as efficiently and cost effective as possible given timing and travel requirements. Valid expenses typically include parking, meals, lodging, photocopying, communication costs, airfare, mileage, and/or automobile rental.
3. All invoices submitted by Trustwave are due and payable within thirty (30) days of the date of the invoice. If Client fails to pay an invoice within the thirty (30) days, Client shall pay interest on such invoices at the rate of 1.5% per month. All fees are quoted and payable in US dollars and exclusive of taxes. In addition to any other rights and remedies, if payment is not received within forty-five (45) days from the date of the invoice, Trustwave reserves the right to disable Client's access to the TrustKeeper portal and or other services.
4. Proposals are valid for up to sixty days from the date on the cover page.
5. Client shall pay the fees annually upfront prior to the commencement of each year of the term.

PROJECT DELIVERABLES

Deliverable	Description
Vulnerability Scan Report	[redacted]
Compliance Certificate from TrustKeeper	[redacted]
Trusted Commerce Seal	[redacted]
External Penetration Test Report	[redacted]
Internal Penetration Test Report	[redacted]

PREREQUISITES

Dependencies and Assumptions

This Agreement was developed based on the following dependencies and assumptions, which if not accurate or adhered to, may require a change in the scope of services. Any change in services and fees will be mutually agreed to in writing by both parties. The dependencies and assumptions include:

1. Trustwave shall not begin to provide the Services as described in this Statement of Work (SOW) until Client has returned this signed SOW and a Purchase Order (PO) for the total amount of the Services selected (full contract amount). All terms and conditions included in a PO or submitted with a PO shall be null and void for all purposes.
2. Client's Primary Contact (PC), as identified below or their designee must be available to Trustwave during the entire engagement. The representative must have sufficient authority to schedule testing and address any issues that may arise.
3. Client will provide Trustwave with sufficient information to evaluate compliance for all PCI DSS requirements. Client is solely responsible for providing access to and coordinating any required interviews or testing with Client's third parties or service providers.
4. If needed, Client will provide resources and information as requested to enable Trustwave's consultants to sufficiently develop documentation consistent with PCI Information Security Policy requirements. This will include access to personnel who can provide information related to the business operations, organizational structure, network architecture, security controls, disaster recovery and general daily operational processes and procedures.
5. Client shall provide and coordinate Trustwave's onsite access to the systems being tested as necessary. Before any system access is allowed, Client shall inform Trustwave in writing and in advance of any security and access standards or requirements.
6. During testing, the configuration of Client's network will be kept as stable as possible (i.e., no new systems or configuration changes). If changes are required, then Client shall inform Trustwave, and a mutually acceptable testing schedule shall be agreed upon.

Contact Information

Contact **South Carolina Department of Revenue**

Name: ______________________________

Title: ______________________________

Phone/Fax: ______________________________

E-mail Address: ______________________________

Billing Address: ______________________________

Assessment Site Address
(if different): ______________________________

TERMS AND CONDITIONS

1. The parties agree to amend the Agreement to include the following provision. In the event the provision already exists in the Agreement in some form, the parties agree to amend such provision to read as follows.

   TRUSTWAVE and CLIENT hereby confirm that the provisions of a mutual non-disclosure agreement between TRUSTWAVE and CLIENT, if executed, shall be in full force and effect and apply to all information furnished by either party in connection the services. In addition, Trustwave is contractually bound to provide this agreement and any amendments to the Payment Card Industry Security Standards Council ("PCI SSC"), and to provide Client's reports, attestation of compliance, work papers and information related to the Services to the PCI SSC, Client's Acquirer, if applicable, and the payment card associations. As such, Client authorizes TRUSTWAVE to release this agreement and any amendments to the PCI SSC, and to release all such Client reports, work papers, and information related to the Services to the Client's merchant acquiring bank, if applicable, PCI Security Standards Council and the payment card associations. TRUSTWAVE shall have the right to retain a copy of client's information solely as necessary for TRUSTWAVE to comply with the PCI SSC data retention requirements for QSA's.

2. Neither party may assign, delegate nor otherwise transfer the rights or obligations associated with this Agreement, in whole or in part, without the prior written consent of the other party; provided however, no written consent shall be required to assign this Agreement to any parent or the wholly owned subsidiary of the party. Furthermore, no written consent shall be required for Trustwave to assign this Agreement to its successor as a result of a merger, acquisition, sale, transfer or other disposition of all or substantially all of its assets. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties, their respective successors and permitted assigns.

3. Annualized services must be used each year during the term and cannot be used and/or credited in subsequent years.

4. All notices, consents, and approvals required by this Agreement may be sent by electronic mail

5. All other terms and conditions shall remain in full force and effect.

{SIGNATURE PAGE FOLLOWS}

SIGNATURES

IN WITNESS WHEREOF, the Parties below have executed this agreement as of the date indicated below.

Trustwave: As a duly elected officer authorized to enter into Agreements and contracts on behalf of Trustwave, I herby provide and accept this Addendum for the designated services and term as accepted by Client:

Signature: ______________________

Print Name: ______________________

Title: ______________________

Effective Date: ______________________

South Carolina Department of Revenue: As a duly authorized representative with the authority to enter into agreements and contracts on behalf of Client, I hereby accept this Addendum for the designated services and term as initialed below:

Tick requested services and desired term:

Requested Service	**1 Year Term**	**3 Year Term**	**5 Year Term**
Compliance Validation Service Package			19,320.00
Managed IPS Service			15,000.00
DLP Discover			3,999.00
			38,319.00/yr.

Signature: Michael Garon 6/29/11

Print Name: Michael D. Garon

Title: Sr. Administrator + CIO

Effective Date: 7/1/11 – 6/30/16

Ver 03MAY11

Trustwave

Trustwave®
Information Security & Compliance

Managed Security Services

Presented To:

South Carolina Department of Revenue

June 30, 2009

Prepared By:

Tony Siegel
TSiegel@trustwave.com
312-873-7276

Exhibit A – Statement of Work to the Master Services Agreement dated 6-30 Rc, 2009

Table Of Contents

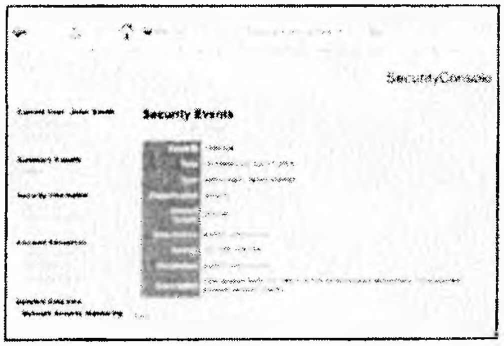
PROPOSAL OVERVIEW 1
TRUSTWAVE OVERVIEW 2
Corporate Overview 2
SERVICES AGREEMENT 3
Intrusion Prevention Service 3
Setup Services 3
1.1. Information Collection and Policy Development 3
1.2. Appliance Configuration and Testing 3
Ongoing Services 3
2.1. Remote Management and Maintenance of the CPE. 3
2.2. Ongoing Maintenance of the Installed Programs 3
DETAILED PRICING SCHEDULE 4
Intrusion Prevention Service 4
CLIENT OBLIGATIONS 5
SERVICE LEVEL AGREEMENT 7
Service Level Goals 7
Intrusion Prevention Service 7
Service Level Measurement and Remedies 7
SIGNATURES 9
Initial requested services and desired term 9

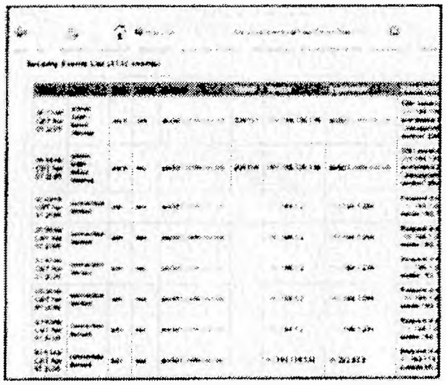
PROPOSAL OVERVIEW

Based upon conversations with the client, South Carolina Department of Revenue is seeking a company to provide Managed Security Services. With its experience providing such services for many clients and data security and network monitoring expertise, Trustwave is qualified to provide the following managed services:

- ❑ **Intrusion Prevention Systems (IPS):**
  - ➢ Prevents malicious traffic from compromising a network environment
  - ➢ Ceaseless expert inquiry ensures legitimate traffic is not dropped

All services include secure Web portal for viewing reports, tickets, changes and notification information





TRUSTWAVE OVERVIEW

Corporate Overview

Trustwave is the leading provider of data security and compliance solutions to businesses in the payment card industry including acquirers, service providers, third-party providers, and merchants. A summary of TRUSTWAVE's payment industry credentials and security experience is listed below:

- **Compliance Management Leader** - TRUSTWAVE has worked with more than 2,000 Level 1, 2 and 3 merchants and service providers; and more than 25,000 Level 4 merchants since the Visa CISP program launched in June 2001. Authorized by all the major card associations – Visa, MasterCard, Discover, American Express and JCB – TRUSTWAVE provides vulnerability scanning, on-site security assessments, computer forensic services and compliance management programs that help organizations validate their compliance with the Payment Card Industry (PCI) Data security Standard.

- **Data Security Experts** - TRUSTWAVE professionals have delivered information security technology solutions to the Fortune 5000, small businesses and government agencies for more than 10 years. We have more than 50 QDSP-certified security professionals and many of our security consultants have worked at government agencies such as the National Security Agency (NSA).

- **Innovative Solutions** - TRUSTWAVE offers the latest solutions to help secure data and validate *compliance:*

  - ***TrustKeeper®***—TRUSTWAVE's enterprise compliance portal—supports more than 25,000 merchants with compliance management solutions. TrustKeeper clients can validate compliance with HIPAA, GLBA, SOX, FISMA and ISO17799.

  - TRUSTWAVE also now offers a first-of-its-kind, adaptive intrusion prevention system (IPS) that uses an asset-centric approach to block malicious traffic based on a system's vulnerabilities—dramatically reducing false positives.

  - To date TRUSTWAVE has validated the majority of payment applications that comply with Visa's Payment Application Best Practices (PABP) through its ***TrustedApp®*** service.

  - TRUSTWAVE's ***TrustSentry®*** suite includes a comprehensive array of managed security solutions: intrusion detection and prevention, firewall management and monitoring, VPN, anti-virus, authentication, and vulnerability scanning. TrustSentry also integrates support-ticketing, online help, and real-time reporting into its intuitive management console.

Global Organization - Headquartered in Chicago, TRUSTWAVE holds offices throughout North America. Its international arm, Trustwave Limited, is based in London with offices throughout Europe and Asia. This expansion allows TRUSTWAVE to continue to combine industry expertise with innovative products and match them with organizations around the world in need of information security and compliance management solutions.

SERVICES AGREEMENT

This is a Statement of Work, dated as of the date executed below, to and governed by the Master Services Agreement ("MSA"), by and between Trustwave Holdings, Inc. ("Trustwave") and SC Dpt. of Revenue ("Client"), dated 6-30-09. Trustwave desires to provide additional Services, as identified below to Client, and Client wishes to receive such services pursuant to the terms and conditions, unless otherwise noted below, of the Agreement.

[redacted]

[redacted]

1. [redacted]

a. [redacted]

1.2. [redacted]

a. [redacted]

b. [redacted]

[redacted]

2.1. [redacted]

a. [redacted]

b. [redacted]

c. [redacted]

d. [redacted]

e. [redacted]

f. [redacted]

g. [redacted]

2.2. [redacted]

[redacted]

DETAILED PRICING SCHEDULE

Intrusion Prevention Service

TRUSTWAVE Service	1-Year Term 7/01/09 thru 6/30/2010
Managed Intrusion Prevention (TS-100)	$1,700/mo.

CLIENT OBLIGATIONS

a) [redacted]

b) [redacted]

i) [redacted]

ii) [redacted]

iii) [redacted]

iv) [redacted]

(1) [redacted]

(2) [redacted]

(3) [redacted]

(4) [redacted]

(5) [redacted]

v) [redacted]

vi) [redacted]

vii) [redacted]

viii) [redacted]

ix) [redacted]

x) [redacted]

xi) [redacted]

xii) [redacted]

xiii) [redacted]

xiv) [redacted]

SERVICE LEVEL AGREEMENT

[redacted]

a. [redacted]

b. [redacted]

c. [redacted]

[redacted]

a) [redacted]

b) [redacted]

- [redacted]

c) [redacted]

d) [redacted]

e) [redacted]

[redacted]

{Signature Pages Follow}

SIGNATURES

IN WITNESS WHEREOF, the Parties below have executed this agreement as of the date indicated below.

Trustwave: As a person authorized to enter into Agreements and contracts on behalf of Trustwave, I herby provide and accept this Agreement for the designated services and term as accepted by Client:

Signature: ____________________

Print Name: ____________________

Title: ____________________

Effective Date: ____________________

CLIENT: As a person authorized to enter into agreements and contracts on behalf of Client, I hereby accept this Agreement for the designated services and term as initialed below:

Initial requested services and desired term

TRUSTWAVE Service	1-Year Term
Managed Intrusion Prevention (TS-100)	

Signature: Terry Ellen Garber

Print Name: Terry Ellen Garber

Title: Manager, New Application Development

Effective Date: 7-1-09 to 6-30-10

Addendum to the Master Service Agreement dated June 30, 2009

Presented To:

South Carolina Department of Revenue

Prepared By:

Carol Reif
Creif@trustwave.com
312.873.7272

ADDENDUM

This is an Addendum, dated as of the date executed below, to and governed by Master Services Agreement (MSA or "Agreement"), by and between Trustwave Holdings, Inc. ("Trustwave") and South Carolina Department of Revenue ("Client"), dated June 30, 2009. TRUSTWAVE desires to provide additional Services, as identified below to Client, and Client wishes to receive such services pursuant to the terms and conditions, unless otherwise noted below, of the Agreement.

Purpose and Start Date of Addendum

The purpose of this Addendum is to fully replace the IPS services set forth in the Addendum dated July 1, 2011 with the services listed below. All other terms and conditions of the Addendum shall remain in force and full effect. The services under this Addendum shall commence as of the start date of this Addendum.

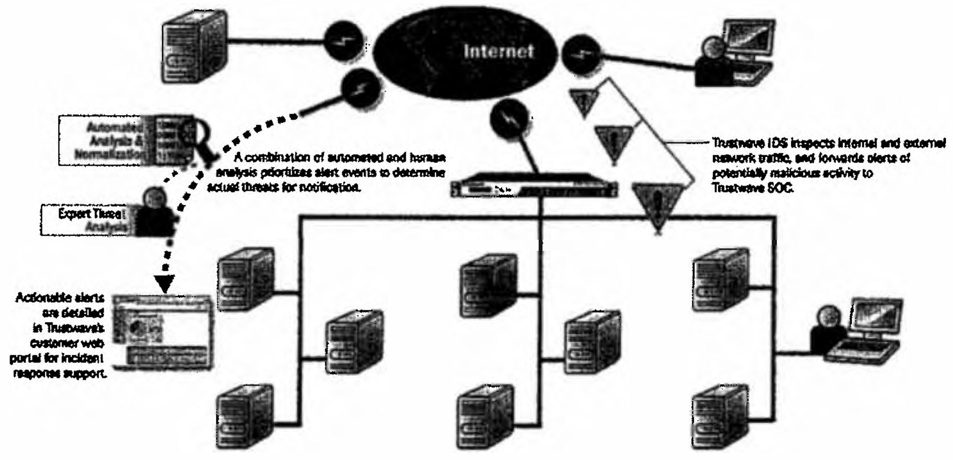
Statement of Work

Managed IDS Service

Trustwave's managed intrusion detection system (IDS) services monitor the effectiveness of control systems by monitoring for evidence of attacks. Trustwave's 24x7x365 network security engineers will manage IDS sensors, analyze the events and take action in case of an actual threat. Trustwave will monitor the events on the SC Department of Revenue network to identify evidence of suspicious activity and filter out false positives so that SC Department of Revenue is notified only of actual threats. Through Trustwave's Customer Portal portal, SC Department of Revenue will have 24x7 online access to suspect activity and reporting. To assist with internal control and compliance requirements, a record of all attack events and their subsequent analyses is automatically posted for SC Department of Revenue's review and to support audit documentation requirements.

Trustwave's managed intrusion detection service includes:

- ☐ IDS Appliance
- ☐ Installation, Baselining and Tuning
- ☐ 24x7 Monitoring
- ☐ Regular Attack Signature Updates
- ☐ Technical Support
- ☐ 24x7 Reporting


Internet
Automated Analysis & Normalization
A combination of automated and human analysis prioritizes alert events to determine actual threats for notification.
Trustwave IDS inspects internal and external network traffic, and forwards alerts of potentially malicious activity to Trustwave SOC.
Expert Threat Analysis
Actionable alerts are detailed in Trustwave's customer web portal for incident response support.

Detailed Pricing Schedule

Trustwave Service	5-Year Term
Managed IDS Service (offered at the same rate as IPS)	$15,000/yr.

[redacted]

ii. [redacted]

c. [redacted]

2.2. [redacted]

[redacted]

Service Level Measurement and Remedies

[redacted]

a) [redacted]

b) [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

c) [redacted]

d) [redacted]

e) [redacted]

[redacted]

SERVICE LEVEL AGREEMENT

Intrusion Detection Service

Service Level Goals

[redacted]

a. [redacted]

b. [redacted]

c. [redacted]

d. [redacted]

Setup Services

1.1. [redacted]

a. [redacted]

b. [redacted]

1.2. [redacted]

a. [redacted]

b. [redacted]

Ongoing Services

2.1. [redacted]

[redacted]

a. [redacted]

b. [redacted]

i. [redacted]

[redacted]

Change Control Procedures

[redacted]

{Signature Pages Follow}

SIGNATURES

IN WITNESS WHEREOF, the Parties below have executed this agreement as of the date indicated below.

Trustwave: As a duly elected officer authorized to enter into Agreements and contracts on behalf of Trustwave, I herby provide and accept this Addendum for the designated services and term as accepted by Client:

Signature: Robert J McCullen

Print Name: Robert J. McCullen

Title: CEO

Effective Date: 10/28/11

Trustwave
MB

CLIENT: As a duly authorized representative with the authority to enter into agreements and contracts on behalf of Client, I hereby accept this Addendum for the designated services and term as initialed below:

Signature: Michael D Garon

Print Name: Michael D. Garon

Title: Sr. Administrator / CIO

Trustwave®
Information Security & Compliance

Trustwave Managed Services
Master Services Agreement

Presented To:

South Carolina Department of Revenue

June 30, 2009

Prepared By:

Tony Siegel
TSiegel@Trustwave.com
312-873-7276

Table of Contents

MANAGED SERVICE MASTER SERVICE AGREEMENT 1

Administrative Contacts 1

Technical Contacts 1

TERMS AND CONDITIONS 2

Definitions 2

Effective Date 2

TRUSTWAVE Obligations 2

Client Obligations 3

Compensation 3

Proprietary Rights 3

Confidentiality 4

Termination Events 4

Warranties and Disclaimer 5

Limitation of Liability 5

Miscellaneous 6

MANAGED SERVICE MASTER SERVICE AGREEMENT

This MASTER SERVICE AGREEMENT (the "Agreement") is entered into by Trustwave Holdings, Inc., a Delaware corporation ("TRUSTWAVE"), with a principal address of 70 W. Madison Street , Suite 1050, Chicago, IL 60602, and the client identified below (the "Client"). The parties agree as follows:

Administrative Contacts

INSERT CLIENT Name	Ms. Jamie Polick
Title	Director of Sales Operations
Client's Full Legal Name	Trustwave Holdings, Inc.
Street Address 1	70 W. Madison Street
Street Address 2	Suite 1050
City, State Zip	Chicago, IL 60602
Tel. No.	Tel. No. 312-873-7451
Fax No.	Fax No. 312-443-1620

Technical Contacts

CLIENT Name	
Title	Director of Managed Services
Street Address 1	612 W. Main Street
Street Address 2	Suite 200
City, State Zip	Madison, WI 53703
Tel. No.	Tel. No 608-294-6940
Fax No.	Fax No. 608-294-6950

In consideration of the mutual obligations assumed under this Agreement, TRUSTWAVE and Client agree to the Terms and Conditions attached hereto and incorporated by reference and represent that this Agreement is executed by duly authorized representatives as of the dates below.

AGREED BY:

[CLIENT]	**Trustwave Holdings, Inc.**
By: Terry Ellen Garber	By:
Name: Terry Ellen Garber	Name:
Title: Manager, New Application Development	Title:
Date: 6-30-09	Date:

TERMS AND CONDITIONS

Definitions.

a) "Confidential Information" means this Agreement and all its Attachments, any addenda hereto signed by both parties, all software, documentation, information, data, drawings, benchmark tests, specifications, trade secrets, object code and machine-readable copies any software and any other proprietary information supplied to Client by TRUSTWAVE to include access to TRUSTWAVE websites and service portals and the content therein, including all items defined as "confidential information" in any other agreement between Client and TRUSTWAVE whether executed prior to or after the date of this Agreement.

b) "Access Control Policy" means a description network traffic flows permitted by Client including, but not limited to, a description of specific network ports and/or addresses that will be denied or permitted access to Client's Site and that will be monitored.

c) "Authorized Persons" means the person or persons (not to exceed three) designated by Client on the Order Form to coordinate the performance of Client's obligations hereunder; and any decision of or direction given to TRUSTWAVE by the Authorized Person[s] may be relied on by TRUSTWAVE and shall be binding on Client.

d) "Client Premises Equipment" or "CPE" means any equipment or appliances provided to Client by TRUSTWAVE and used by TRUSTWAVE for provision of the Services.

e) "Effective Date" means the date that the later of Client or TRUSTWAVE has signed this Agreement.

f) "Incident" means any Security Breach, operator error, failure of the Installed Programs or the CPE, or otherwise.

g) "Installed Programs" means the software programs installed by TRUSTWAVE on the CPE.

h) "Network Operations Center" or "NOC" means TRUSTWAVE's facilities from which Client's networks are monitored or certain Services are provided.

i) "Purchase Order" means the Purchase Order or Purchaser Order Exemption Form attached hereto, as the same may be amended in writing by Client and TRUSTWAVE from time to time.

j) "Security Breach" means an abuse of privilege, i.e. when a user performs an action that is not permitted according to the Access Control Policy, including but not limited to break-ins or attempted break-ins to Client's Site.

k) "Service Date" means the date TRUSTWAVE commences delivery of the Services or 30 (thirty) days after Effective Date, whichever is earlier.

l) "Service Level Goals" means the goals for the delivery of the Services as set forth in Exhibit B.

m) "Service Level Agreement" means the terms set forth in Exhibit C.

n) "Service Period" means the calendar month in which the Service is provided.

o) "Site" means Client's network specified in the Statement of Work Form.

p) "System" means a computer, computer system, or computer network.

q) "Monitored Device" means any System specified on a Statement of Work with regard to the Network Security Monitoring service.

r) "Data Conduit" means the system interconnection configured and operated for the purpose of transferring data from Monitored Devices to the NOC.

s) "Rampart™ Data Conduit" means a Data Conduit that utilizes TRUSTWAVE's Rampart™ CPE.

t) "VPN Data Conduit" means a Data Conduit implemented using a Virtual Private Network (VPN) technology that is configured to a specification provided by TRUSTWAVE.

Effective Date

This Agreement shall become effective as of the Effective Date and shall have an initial term of three (3) years and shall automatically renew for additional one (1) year terms unless one of the parties provides the other written notice of its intent not to renew at least ninety (90) days prior to such renewal.

TRUSTWAVE Obligations

a) TRUSTWAVE shall provide to Client the services and deliverables (collectively the "Services") described in the attached Exhibit A, Statement of Work. Additional Statements of Work shall be consecutively number (e.g. A, A-1, A-2, etc.).

b) TRUSTWAVE shall use reasonable commercial efforts to meet the Service Level Goals described in the attached Exhibit A, Statement of Work(s).

Client Obligations

a) Client shall provide, perform, and make available to TRUSTWAVE, at Client's expense within 30 (thirty) days of the Effective Date , the resources and actions and information set forth in the attached Exhibit A, Statement of Work, and such other additional resources and actions and information, as TRUSTWAVE may from time to time reasonably request in connection with TRUSTWAVE's performance of the Services.

b) Client understands and acknowledges that TRUSTWAVE will rely upon the accuracy of any information provided by Client and that TRUSTWAVE's performance is dependent on Client's timely and effective satisfaction of all of Client's responsibilities hereunder and timely decisions and approvals by Client.

c) Client shall pay all insurance, shipping, and handling charges, including without limitation, custom charges, taxes, and VAT.

Compensation

a) Fees. In consideration of the Services provided hereunder, Client shall pay to TRUSTWAVE the fees set forth in the Statement of Work and Purchase Order, if necessary. TRUSTWAVE may adjust the fees on each anniversary of the Effective Date provided it gives Client written notification of the same not less than thirty (30) days prior to such adjustment. Travel and expenses are not included in the fees and will be billed separately as approved.

b) Payment Terms. The Setup Fee is due and payable upon execution of this Agreement. The invoice for the Service Fee for the initial Service Period (the calendar month in which the Service Date falls) will be prorated according to the Service Date. Thereafter, invoices for the Service Fee will be sent in advance of the start of the Service Period. All such invoiced amounts (except the Setup Fee as noted above) shall be due and payable within fifteen (15) days after the date of invoice. The Fee for the Assessment Services and subsequent Setup Fee(s) is due and payable within fifteen (15) days after the date of invoice. All fees quoted and payments shall be in U.S. Dollars .

c) Invoicing. Statement(s) of Work with a value of $12,000.00 or less per year shall be paid upon execution thereof. Trustwave will begin invoicing for the Services fifteen (15) days after the execution of the Agreement. However if the Services do not commence within such time solely as a result of Trustwave, invoicing for the Services will begin thirty (30) days after the execution of this Agreement.

d) Late Payment. Any amounts not paid within thirty (30) days of the date due shall accrue interest at the rate of one and one-half percent (1.5%) per month or the maximum rate permitted by applicable law, whichever is less, determined and compounded on a daily basis from the date due until the date paid. If payment is not received within forty-five (45) days from the date of the invoice, TRUSTWAVE reserves the right to disable Client's access to the TrustKeeper portal and or other services.

e) Taxes. Client shall be responsible for any taxes (except for taxes on TRUSTWAVE's income), such as sales, use or excise taxes, and similar charges of any kind imposed by any federal, state or local governmental entity for Services provided under this Agreement.

Proprietary Rights

a) TRUSTWAVE Technology. All software, data processing systems or mechanisms, computer code, report templates, CPE, trade secrets, know-how, processes, inventions, discoveries, concepts, improvements, and original works of authorship and derivative works thereof that TRUSTWAVE has prepared, developed, acquired for the purpose of providing the Services (the "TRUSTWAVE Technology") to include websites and services portal and their content shall be the sole property of TRUSTWAVE or its licensors. Except as otherwise expressly provided herein, Client shall not acquire any rights in any TRUSTWAVE Technology as a result of receiving the Services.

b) Data. In the course of providing the Services, TRUSTWAVE will collect information relating to activities on Client's network (the "Data") including, but not limited to, network configuration, TCP/IP packet headers and contents, log files, malicious codes, and Trojan horses. TRUSTWAVE retains the right to use the Data or aggregations thereof for any reasonable purpose, provided such data does not contain information identifying Client or disclose any of Client's confidential information.

c) Client agrees that nothing in this Agreement will impair TRUSTWAVE's right to provide to others services or deliverables substantially similar to, or performing the same or similar functions as, the Services under this Agreement.

d) Trademarks and Logo. Client shall not have any rights to use TRUSTWAVE's trademarks, service marks or logos for any other purpose without the prior written approval of TRUSTWAVE's legal department.

Confidentiality

a) Client acknowledges that the Confidential Information constitutes valuable trade secrets and Client agrees that it shall use Confidential Information solely in accordance with the provisions of this Agreement and will not disclose, or permit to be disclosed, the same, directly or indirectly, to any third party without TRUSTWAVE's prior written consent. Client agrees to exercise due care in protecting the Confidential Information from unauthorized use and disclosure. However, Client bears no responsibility for safeguarding information that is publicly available, already in Client's possession and not subject to a confidentiality obligation, obtained by Client from third parties without restrictions on disclosure, independently developed by Client without reference to Confidential Information, or required to be disclosed by order of a court or other governmental entity.

b) TRUSTWAVE acknowledges that, in the course of its performance of this Agreement, it may become privy to certain information that Client deems proprietary and confidential. TRUSTWAVE agrees to treat all such information that is identified as proprietary and confidential in a confidential manner and will not disclose or permit to be disclosed the same, directly or indirectly, to any third party without Client's prior written consent. However, TRUSTWAVE bears no responsibility for safeguarding information that is publicly available, already in TRUSTWAVE's possession and not subject to a confidentiality obligation, obtained by TRUSTWAVE from third parties without restrictions on disclosure, independently developed by TRUSTWAVE without reference to such information, or required to be disclosed by order of a court or other governmental entity.

c) The parties acknowledge that either party's breach of its obligations of confidentiality may cause the other party irreparable injury for which it would not have an adequate remedy at law. In the event of a breach, the non-breaching party shall be entitled to seek injunctive relief in addition to any other remedies it may have at law or in equity.

d) Notwithstanding the foregoing, TRUSTWAVE shall have the right to utilize Client's name and address in their "Client List" and other marketing materials without additional compensation to Client provided that such usage is in the reasonable and normal marketing activities of TRUSTWAVE, that such usage shall in no way be derogatory in nature, that such usage does not result in disclosure of Client's confidential information.

e) **Incidental Fees**. Client shall immediately notify TRUSTWAVE if Client knows or has reason to believe that TRUSTWAVE has been or will be required, as a result of activity arising out of or related to this Agreement or the services contemplated hereunder, by any court or administrative agency of the United States or any state or by any legal process to respond to any subpoena, search warrant, discovery or other directive under the authority of such court, administrative agency, governmental inquiry or process in connection with any proceeding or investigation in which Client or any of its Affiliates, officers, directors, agents, employees, or subcontractors is involved. Whether or not such notice is given by Client, Client shall directly assist TRUSTWAVE in TRUSTWAVE's attempt to reduce the burdens of compliance with any such directive, and Client shall reimburse any and all reasonable expenses incurred by TRUSTWAVE and its Affiliates in complying with any such directive, including, but not limited to, attorneys' fees and TRUSTWAVE's outside counsel attorneys' fees for representation and advice, travel and lodging expenses and an hourly labor rate of $275 per hour for all time spent by TRUSTWAVE in responding to such matters.

Termination Events

a) This Agreement or Service may, by written notice, be terminated by a party if any of the following events ("Termination Events") occur:

   i) TRUSTWAVE is in material breach of any term, condition or provision of this Agreement, which breach, if capable of being cured, is not cured within thirty (30) days after Client gives TRUSTWAVE written notice of such breach; or

   ii) As to any Service TRUSTWAVE delivers to Client from a third-party vendor, such vendor removes or disables access to all or any portion of such Service, ceases to do business or otherwise terminates its business operations; or

   iii) Client fails to pay any amount due TRUSTWAVE within thirty (30) days after TRUSTWAVE gives Client written notice of such nonpayment; or

   iv) Client is in material breach of any nonmonetary term, condition or provision of this Agreement, which breach, if capable of being cured, is not cured within thirty (30) days after TRUSTWAVE gives Client written notice of such breach; or

   v) Client (i) terminates or suspends its business, (ii) becomes insolvent, admits in writing its inability to pay its debts as they mature, makes an assignment for the benefit of creditors, or becomes subject to direct control of a trustee, receiver or similar authority, or (iii) becomes subject to any bankruptcy or insolvency proceeding under federal or state statutes.

b) If any Termination Event occurs, termination will become effective immediately or on the date set forth in the written notice of termination. Termination of this Agreement will not affect the provisions regarding Client's or TRUSTWAVE's treatment of Confidential Information, provisions relating to the payment of amounts due, or provisions limiting or disclaiming TRUSTWAVE's liability, which provisions will survive termination of this Agreement.

c) Within ten (10) business days after the date of termination or discontinuance of this Agreement for any reason, Client agrees to return, at its sole expense without setoff to any fees owed, any CPE(s) to TRUSTWAVE. Client shall retain the risk of loss until such CPE is delivered to TRUSTWAVE's premises. Client shall be solely responsible for, and shall reimburse TRUSTWAVE for, any damage caused to the CPE while it is installed at Client's facilities, except to the extent such damage is caused by TRUSTWAVE personnel. If the CPE(s) are not timely returned or are not in the same condition in which received by Client (except for normal wear and tear), Client agrees to pay a damage fee of $5,000 per CPE.

d) If Client terminates this Agreement for any reason, Client agrees to pay TRUSTWAVE within 30 days for all services performed by TRUSTWAVE up to the date of cancellation that have not previously been paid. Additionally, if Client terminates this Agreement other than for cause, then Client shall pay to TRUSTWAVE, as a cancellation fee and not as a penalty, an amount equal to the sum of the monthly service charges for the remainder of the Term of the agreement.

Warranties and Disclaimer

a) By TRUSTWAVE. TRUSTWAVE warrants that the Services provided under this Agreement shall be performed with that degree of skill and judgment normally exercised by recognized professional firms performing services of the same or substantially similar nature. The exclusive remedy for any breach of the foregoing warranty shall be that TRUSTWAVE, at its own expense, and in response to written notice of a warranty claim by Client within 90 days after performance of the Services at issue, shall, at its own option, either (1) re-perform the Services to conform to this standard; or (2) refund to Client amounts paid for non-conforming Services.

b) By Client. Client represents and warrants to TRUSTWAVE that it has the right to use, disclose and disseminate the information, specifications and data that it has provided or will provide to TRUSTWAVE in order for TRUSTWAVE to perform the Services and to grant TRUSTWAVE access to the Client's IP address(es) as identified and provided by Client to scan for open ports and other possible security vulnerabilities. Client further represents and warrants that possession and use of that information, specifications and data by TRUSTWAVE under the terms and conditions of this Agreement will not constitute an infringement upon any patent, copyright, trade secret, or other intellectual property right of any third party,

c) CPE Warranty. In the event of a defect in the materials or workmanship of the CPE, Client shall have the right to return such defective CPE to TRUSTWAVE, and TRUSTWAVE shall, at TRUSTWAVE's election and expense, either repair or replace such defective CPE. Client agrees to pay for shipping charges related to the replaced CPE. Client shall be solely responsible for all costs associated with repairing or replacing any CPE damaged by accident; unusual physical, electrical or electromagnetic stress; neglect; misuse; failure of electric power, air conditioning or humidity control; causes other than ordinary use; or any damage resulting from a breach of Client's obligations hereunder.

d) TRUSTWAVE does not warrant that the CPE or Services are offered without defect or error, or that the operation of the CPE or availability of the Services will be uninterrupted or error-free. Furthermore Client acknowledges and understands that the monitoring for availability of dynamically addressed CPE devices may result in a greater time window for device outage detection.

e) EXCEPT AS EXPRESSLY SET FORTH HEREIN, TRUSTWAVE SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED STANDARDS, GUARANTEES, OR WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WARRANTIES OF NON-INFRINGEMENT OR ANY WARRANTIES THAT MAY BE ALLEGED TO ARISE AS A RESULT OF CUSTOM OR USAGE. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS AGREEMENT TRUSTWAVE DISCLAIMS ANY WARRANTY, RESPONSIBILITY, OR LIABILITY FOR THE FUNCTIONALITY OF THE CLIENT'S HARDWARE, SOFTWARE, FIRMWARE, OR COMPUTER SYSTEMS.

Limitation of Liability

a) TRUSTWAVE SHALL NOT BE LIABLE TO CLIENT FOR (1) ANY ACTS OR OMISSIONS WHICH ARE NOT THE RESULT OF TRUSTWAVE'S GROSS NEGLIGENCE, RECKLESSNESS OR WILLFUL MISCONDUCT, (2) ANY AMOUNTS IN EXCESS OF ANY FEES PAID TO TRUSTWAVE BY CLIENT HEREUNDER, (3) ANY OUTAGES OR SLOW DOWNS OF CLIENT'S COMPUTER SYSTEMS RESULTING FROM THE PERFORMANCE OF ANY SERVICES UNLESS SUCH ARE THE RESULT OF TRUSTWAVE'S GROSS NEGLIGENCE, RECKLESSNESS OR WILLFUL MISCONDUCT, OR (4) ANY LOSSES, COSTS, DAMAGES OR EXPENSES INCURRED BY CLIENT RESULTING FROM THE PERFORMANCE OF ANY TEST, UNLESS SUCH ARE THE RESULT OF TRUSTWAVE'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

b) THIS AGREEMENT IS A SERVICE AGREEMENT, AND EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, TRUSTWAVE DISCLAIMS ALL OTHER REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES REGARDING QUALITY, SUITABILITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE (IRRESPECTIVE OF ANY COURSE OF DEALING, CUSTOM OR USAGE OF TRADE) OF ANY SERVICES OR ANY GOODS OR SERVICES PROVIDED INCIDENTAL TO THE SERVICES PROVIDED UNDER THIS AGREEMENT.

c) NOTWITHSTANDING ANY PROVISION IN THIS AGREEMENT, IN NO EVENT WILL TRUSTWAVE BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF USE, BUSINESS INTERRUPTION, LOSS OF DATA, COST OF COVER OR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND IN CONNECTION WITH OR ARISING OUT OF THE FURNISHING, PERFORMANCE OR USE OF THE SERVICES PERFORMED HEREUNDER, WHETHER ALLEGED AS A BREACH OF CONTRACT OR TORTIOUS CONDUCT, INCLUDING NEGLIGENCE, EVEN IF TRUSTWAVE HAS BEEN

ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ADDITION, TRUSTWAVE WILL NOT BE LIABLE FOR ANY DAMAGES CAUSED BY DELAY IN DELIVERY OR FURNISHING THE SERVICES. TRUSTWAVE'S LIABILITY UNDER THIS AGREEMENT FOR DAMAGES WILL NOT, IN ANY EVENT, EXCEED THE FEES PAID BY CLIENT TO TRUSTWAVE UNDER THIS AGREEMENT IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING ANY CLAIM.

THE PROVISIONS OF THIS SECTION 10 ALLOCATE RISKS UNDER THIS AGREEMENT BETWEEN CLIENT AND TRUSTWAVE. CLIENT UNDERSTANDS THAT TRUSTWAVE IS NOT AN INSURER, THAT INSURANCE, IF ANY, SHALL BE OBTAINED BY THE CLIENT AND THAT TRUSTWAVE'S PRICING REFLECTS THE ALLOCATION OF RISKS AND LIMITATION OF LIABILITY SET FORTH HEREIN.

TRUSTWAVE shall incur no liability for good faith reliance on the information provided by authorized persons or resulting from any incident, or action or inaction of Client. Client understands and acknowledges that, by its very nature the performance of the services may result in Client system downtime.

No action arising out of any breach or claimed breach of this agreement or transactions contemplated by this agreement may be brought by either party more than one (1) year after the cause of action has accrued. For purposes of this agreement, a cause of action will be deemed to have accrued when a party knew or reasonably should have known of the breach or claimed breach.

NO EMPLOYEE, AGENT, REPRESENTATIVE OR AFFILIATE OF TRUSTWAVE HAS AUTHORITY TO BIND TRUSTWAVE TO ANY ORAL REPRESENTATIONS OR WARRANTY CONCERNING THE SERVICES. ANY WRITTEN REPRESENTATION OR WARRANTY NOT EXPRESSLY CONTAINED IN THIS AGREEMENT WILL NOT BE ENFORCEABLE.

Miscellaneous

a) Assignment. This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns. Notwithstanding the foregoing, Client shall not transfer or assign any or all of its rights or obligations hereunder without first obtaining the written consent of TRUSTWAVE. Any attempted assignment or transfer made in violation of this Section 11.a. shall be null and void.

b) Force Majeure. The obligations hereunder of each party shall be suspended while and to the extent that such party is prevented from complying herewith in whole or in part by any event beyond the reasonable control of such party.

c) Notices. All notices, consents, and other communications hereunder shall be provided in writing and shall be delivered personally, by registered or certified mail (return receipt requested) or by facsimile to the parties at the addresses on front (or such other address as may have been furnished by or on behalf of such party by like notice):

   i) Communications sent by facsimile shall be deemed effectively delivered upon dispatch.

   ii) Communications sent by registered or certified mail shall be deemed effectively delivered five (5) calendar days after mailing.

d) Relationship. The relationship between the parties to this Agreement shall be that of independent contractors. It is expressly agreed that nothing in this Agreement shall be construed to create or imply a partnership, joint venture, agency relationship or contract of employment. Neither party shall have the authority to make any representation or commitment of any kind, or to take any action that shall be binding on the other party, except as authorized in writing by the party to be bound.

e) Subcontractors. Client expressly consents to TRUSTWAVE's right to use of subcontractors in connection with the performance of Services hereunder, provided that should TRUSTWAVE use subcontractors, it would not relieve TRUSTWAVE of any of its obligations under this Agreement.

f) No Solicitation. During the term and for a period of one (1) year thereafter, CLIENT shall not, directly or indirectly solicit, hire, attempt to solicit or hire, or participate in any attempt to solicit or hire any person who was an employee of TRUSTWAVE or any of its Affiliates. If Client breaches this provision, Client shall pay TRUSTWAVE two times (2X) the salary paid by TRUSTWAVE to such employee so hired. The parties agree that said amount is a reasonable estimate of the costs and expenses that TRUSTWAVE will incur as a result of training and replacing such employee.

g) Communications. Client agrees to receive communications from Trustwave.

h) Waiver. Any waiver of the provisions of this Agreement or of a party's rights or remedies under this Agreement must be in writing to be effective.

i) Severability. If any term, condition, or provision in this Agreement is found to be invalid, unlawful or unenforceable to any extent, the parties shall endeavor in good faith to agree to such amendments that will preserve, as far as possible, the intentions expressed in this Agreement. If the parties fail to agree on such an amendment, such invalid term, condition or provision will be severed from the remaining terms, conditions and provisions, which will continue to be valid and enforceable to the fullest extent permitted by law.

j) Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Illinois, without regard to conflict of laws principles. Each party hereby irrevocably submits to the jurisdiction and venue of the federal and state courts of the State of Illinois for the purpose of any legal or equitable action arising under this Agreement.

k) Venue. Venue for any action arising from the terms of this Agreement shall be in the Illinois and Federal District courts sitting in the City of Chicago, IL.

l) Entire Agreement; Amendment. This Agreement (together with the attachments, forms and exhibits attached hereto) constitutes the entire agreement between TRUSTWAVE and Client regarding the subject matter hereof. All prior or contemporaneous agreements, proposals, understandings and communications between TRUSTWAVE and Client regarding the subject matter hereof, whether oral or written, are superseded by and merged into this Agreement. Neither this Agreement nor any exhibit hereto may be modified or amended except by a written instrument executed by both TRUSTWAVE and Client. The terms of any Client purchase order are accepted for accounting convenience only. No terms or conditions contained in any purchase order shall amend this Agreement or shall otherwise constitute an agreement between the parties.

Trustwave®
Information Security & Compliance

Addendum to the Compliance Validation Service dated September 30, 2005

PRESENTED TO:

South Carolina Department of Revenue

PREPARED BY:

TONY SIEGEL
312-873-7276

PROPRIETARY INFORMATION

This proposal may only be used for evaluating the planned services designated herein, and may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this proposal or the information herein is prohibited without prior written permission of Trustwave.

Addendum

This is an Addendum, dated as of the date executed below, to and governed by the Payment Application Best Practice ("Agreement"), by and between Ambiron TrustWave now known as Trustwave Holdings, Inc. ("Trustwave") and __________ ("South Carolina Department of Revenue"), dated September 30, 2005. TRUSTWAVE desires to provide additional Services, as identified below to South Carolina Department of Revenue, and South Carolina Department of Revenue wishes to receive such services pursuant to the terms and conditions, unless otherwise noted below, of the Agreement.

Purpose of Addendum

The purpose of this Addendum is to renew the services below.

Service Start Date

The services under this Addendum shall commence as of July 01, 2009.

Statement of Work

Compliance Validation Service (CVS)

Trustwave will provide South Carolina Department of Revenue with a Compliance Validation Service designed to manage the overall compliance process and aid in achieving the compliance objectives. A Trustwave consultant will host weekly calls throughout a 4 week period after the initial questionnaire and scan are completed. The purpose of the calls will be to identify areas of non-compliance uncovered in the questionnaire and scan results, develop and assist in managing a remediation plan to address the non-compliance issues, validate policies and procedures, and review network security infrastructure and architecture. Based on our extensive experience and knowledge, typical areas of non-compliance include card data encryption, multi-factor authentication, and system logging. Throughout the project, Trustwave provides comprehensive online support through the TrustKeeper portal that includes self-help and a continually updated FAQ database. In addition, email and multilingual phone support are available during standard business hours to answer any questions regarding PCI compliance or vulnerability scanning results.

To ensure comprehensive and efficient service, the South Carolina Department of Revenue must fulfill their obligations within each item below before progressing to subsequent phases. Failure to do so may require an addendum to this contract that will include additional charges for any time or materials above and beyond those agreed to in this contract. The Compliance Validation Service does not include remediation services. If South Carolina Department of Revenue wishes to receive any remediation services, South Carolina Department of Revenue must specifically select those services.

Project Phases and Chronology

1. Vulnerability Scanning Service

a. **Online Questionnaire:** PCI requires that all merchants and service providers complete the PCI self-assessment questionnaire. The TrustKeeper system provides an easy-to-use portal that satisfies the requirements of all the card associations with self-help and a continuously updated FAQ database. The questionnaire is available in English (American and British), French, Canadian French, Swedish, Greek, Spanish, Japanese, Chinese (Simplified and Traditional).

b. **Scanning:** The automated vulnerability scanning engine within TrustKeeper is a proprietary "Intelligent" scanning solution that has been tested and determined to be PCI compliant. The scanning solution tests for more than 3,000 unique vulnerabilities and is extremely accurate in eliminating false positives. You are entitled to receive monthly scans during the term of the Agreement for up to **(512)** IP addresses.

c. **Reporting:** Through a secure web interface, TrustKeeper provides easy access to concise, auto-generated reports with a high-level summary for executives and managers. The reports will also provide detailed results and remediation action for technicians. Remediation instructions include CVE-linked vulnerability checks and best practices defined by Trustwave consultants.

d. **Security:** Trustwave's TrustKeeper infrastructure is monitored on a 24x7 basis to ensure protection of South Carolina Department of Revenue data. All South Carolina Department of Revenue data is delivered via secure channels.

2. **Support** – Supplied throughout each phase of the project, Trustwave provides comprehensive online support through the TrustKeeper portal that includes self-help and a continuously updated FAQ database. In addition, email and multilingual phone support are available during standard business hours to answer any questions regarding PCI compliance or vulnerability scanning results.

3. Trusted Commerce Security Seal:

With your service, you receive the Trusted Commerce seal. Displaying the Trusted Commerce seal on your Web site will raise recognition of your organization's commitment to payment card security and distinguish your organization as one that is committed to handling payment card data in a secure manner. The seal confirms your enrollment in Trustwave's program to validate compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Once you've achieved compliance, customers that click on the Trusted Commerce seal will view a certificate stating that your organization has completed the required actions for validation of PCI DSS compliance. The seal informs customers that, as a Qualified Security Assessor, Trustwave examined your organization's policies, procedures and technical systems and scanned your payment card environment for vulnerabilities. This statement reassures customers that you protect their payment card information as required by the PCI DSS and reinforces their trust.

4. Trustwave Extended Validation (EV) SSL Certificate

Included with your Compliance Validation Service (CVS), Trustwave will include one Extended Validation (EV) SSL certificate free for one year to help your organization establish a new standard for its Internet reputation and online security.

The Extended Validation (EV) SSL Certificate Standard has been set in place as a joint effort by Certificate Authorities and Web Browser software vendors worldwide to provide for a more secure Internet. With the emergence of a vast array of new exploits, phishing scams and fraudulent activity on the Internet, EV SSL certificates are at the forefront of a new online security initiative. EV certificates enable secure connections, establish business identities, and assist in preventing fraud through a rigorous set of checks and validations previously unmatched with regular certificate processes.

When an EV SSL is presented during an online session, your customer's browser address bar is shaded green to call attention to and promote your Web site's security. Additionally, an EV SSL certificate fulfills a number of e-commerce requirements within the Payment Card Industry Data Security Standard (PCI DSS).

The EV validation process includes legal, physical, operational, domain name and authority validation and demonstrates to consumers that your company is legitimate and underwent thorough validation. Issuing an EV certificate requires thorough investigation, and Trustwave has streamlined the validation process to reduce the time it takes to issue your certificate. While your EV SSL certificate is processed, Trustwave will issue a traditional Organizationally Validated (OV) SSL certificate to be replaced once your EV SSL is issued. Your use of Trustwave's SSL certificates is subject to and governed by the terms and conditions in the applicable Certification Practice Statement(s), Certificate Policy (ies), Subscriber Agreement, and other related documentation.

Trustwave's EV SSL certificates offer security and credibility unmatched by the first generation of SSL certification and feature the following:

- Prominent green bar
- $500,000 Relying Party Warranty
- 256-Bit Digital Encryption
- Free Priority Technical Support
- 128-bit and 40-bit backward compatibility
- Trusted Commerce℠ Web Site Seal
- Free reissues for the life of the SSL Certificate

External Penetration Service

PCI DSS requirement 11.3 requires that penetration tests are conducted at least annually or after any significant change to your network. This service is designed to satisfy the external portion of these requirements, is performed as a non-credentialed test, and includes the following:

a. **Network Mapping:** In the process of moving from general to specific, building an accurate network map of the externally facing devices is a critical task at the beginning of the penetration test. To support this, in many cases SpiderLabs will obtain the network blocks from the South Carolina Department of Revenue. This is typically in the form of a block of Internet addresses provided by one or many Internet Service Providers (ISPs). These addresses are then probed to see if they are in use (not for vulnerabilities at this time). The probes are executed 3 times at different intervals during the first part of the engagement to ensure that no system is missed. The data gathered is used to create a network map of the external environment.

b. **System Identification and Classification:** The network map would not be very useful if the systems located on the network were not identified and classified. Another probe is performed of the systems identified, this time using TCP finger printing, service fingerprinting, and various methods to identify and classify systems and services. The data gathered is used to classify the systems by function. Data gathered about the system helps to determine the classification For example, a system running a particular version of the Apache Web Server as well as BEA Web logic is most likely a web application server. After each system is classified the network map is updated to reflect each system's functionality and operation system. Before the next testing steps begin, SpiderLabs will debrief the South Carolina Department of Revenue's key security contacts on specific system findings and intended target list to be used in the attack phase.

c. **System Vulnerability Identification:** All systems in the target network segment are probed, singularly and in tandem with the other hosts to locate potential vulnerabilities. Using a large working knowledge of exploit techniques, public information, and results of private vulnerability research, the Trustwave Penetration Testers catalog all the potential attack vectors that might be exploitable. Trustwave Penetration Testers devise several attack strategies and commence to exploitation.

d. **System Vulnerability Exploitation:** If the plan of attack devised in the previous step includes any techniques that may impact production systems and infrastructure, the South Carolina Department of Revenue is first advised of the possible system downtime that may arise. At this point it is up the South Carolina Department of Revenue to decide whether or not to proceed with the exploitation. As a rule, any potential vulnerability found is manually investigated, researched, and an attempt is made to exploit. Exceptions to this rule are techniques that will cause a denial of service (DoS) or harm the data on the target system. SpiderLabs will only attempt to exploit a Denial of Service, or alter data on a target if specifically instructed by the South Carolina Department of Revenue in writing. In exploiting vulnerability, SpiderLabs has will make an attempt to either gain unauthorized access to the target system, or extract sensitive data from it. An exploit is considered successful if we were able to achieve either of these objectives. As successful exploitation leads SpiderLabs to systems compromise, SpiderLabs consultants will report the breach to the South Carolina Department of Revenue's key security personnel immediately.

e. **Application Architecture Identification:** Using the classifications previously established Trustwave will use tools and manual intervention to identify if there are specific applications running on dynamic content servers within the target network. When an application server is identified, other systems will be identified within an application server group. This grouping will help identify potential flaws in application trust relationships. This information is vital to the successful identification of application vulnerabilities. In addition to identifying purposeful applications, Trustwave will attempt to discover Backdoors that may be present in the environment.

f. **Application Exploitation:** Application Exploitation is carried out on the Public areas of exposed applications only, such as login fields, search functions, or other publicly accessible areas. For applications that have public user registration functions, Trustwave WILL NOT attempt to create a user and test authenticated areas of the application. Further, Trustwave WILL NOT perform a full Application Penetration Test against any application as part of an External Penetration Test. Trustwave will debrief the South Carolina Department of Revenue's key security contacts on the applications identified, and what will be tested. Trustwave can explain the plan of attack for each system and general techniques that will be used. If the system is a production system, the South Carolina Department of Revenue will be advised of the possible system downtime that may arise. Each application will be tested with many different types of Application Penetration testing techniques related to input validation, business logic, application logic, session management, and login routines.

g. **Compromise:** As systems or applications are compromised, the South Carolina Department of Revenue's key security contacts will be notified. At this time, the South Carolina Department of Revenue contacts are given the opportunity to decide if the particular system should undergo additional tests. If they decide to have Trustwave continue, additional techniques will be used to further penetrate the target system and the environment as a whole. This can include installation of network sniffers, remote management tools, connectivity tools etc. Successful execution establishes a launch point for additional attacks against the environment.

h. **Data Extraction:** Each system that is compromised will be examined for the existence of critical data and files. If SpiderLabs finds such data to be accessible, a sample of this data will be downloaded from the system and securely stored by SpiderLabs until the presentation of deliverables.

i. **Further Compromise:** Once a system has been compromised, there are many trust relationships that can be potentially exploited, or data exposed through a compromise might lead to the compromise of additional systems and applications. Using both data gathered and techniques similar to those used to develop the network map and system classification, SpiderLabs will launch a new stage of discovery against the environment. For example, a web server is compromised. This system is allowed to access a system on the internal network for data storage and retrieval. The internal server can be potentially compromised if vulnerabilities exists that can be exploited from the web server.

The service will be performed on **1 Class C Network** (containing approximately **1** Dynamic Content Web Server). Upon completion of the testing, a report will be provided documenting the findings and include high-level recommendations to assist you in correcting any areas of deficiency. All testing phases will be coordinated with SOUTH CAROLINA DEPARTMENT OF REVENUE to minimize any adverse impact that may occur as a result of the services. We strongly recommend full-disclosure of the testing to all individuals responsible for the network and related services and devices. Although we take precautions to minimize the negative impact on South Carolina Department of Revenue systems, we do not guarantee against service interruptions due the inherent risk of such testing that could result from unpatched systems, unique system configurations and other such issues. We also recommend the establishment of incident response procedures in the event of any adverse impact or disruption of network services. SOUTH CAROLINA DEPARTMENT OF REVENUE assumes full responsibility to backup and/or otherwise protect its data against loss, damage or destruction prior to and during all phases of the proposed services, and to take appropriate measures to respond to any adverse impact of the systems or disruption of service.

Detailed Pricing Schedule

Requested Service	**1-Year Term** **7/01/09 thru 6/30/2010**
Compliance Validation Service (CVS) • TrustKeeper Scanning and Questionnaire- 512 IP Addresses • Remote Consulting for 4 Weeks • Policy & Procedure Review • 1 Trustwave Extended Validation (EV) SSL Certificate for 2 Year • Trusted Commerce Seal	$12,000
External Penetration Test (30 Hours) • 1 Class C Network • 1 Application	$7,500

- South Carolina Department of Revenue shall pay Trustwave at the rate of $250 per hour for any hours in excess of those listed above.
- South Carolina Department of Revenue shall pay all insurance, shipping, and handling charges, including without limitation, custom charges, taxes, VAT.

TERMS AND CONDITIONS

1. The parties agree to amend the Agreement to include the following provision. In the event the provision already exists in the Agreement in some form, the parties agree to amend such provision to read as follows.

TRUSTWAVE and CLIENT hereby confirm that the provisions of a mutual non-disclosure agreement between TRUSTWAVE and CLIENT, if executed, shall be in full force and effect and apply to all Confidential Information furnished by either party in connection with the services. Notwithstanding, Client authorizes Trustwave to disclose (i) only upon subsequent written approval (which, for purposes of this clause, includes email from Client's point of contact), Client's ROC and other compliance reports and information, including compliance status, to Client's merchant acquiring bank, if applicable, and (ii) relevant information to comply with the Payment Card Industry Security Standards Council (PCI SSC) mandatory disclosure requirements as identified below.

PCI SSC Mandatory Disclosure Requirements for Onsite PCI Compliance Assessments: As a Qualified Security Assessor ("QSA") for the PCI SSC, Trustwave is contractually bound by PCI SSC's Qualified Security Assessor Agreement ("QSA Agreement"), a copy of which can be found at www.pcisecuritystandardscouncil.org. The QSA Agreement, inter alia, identifies the terms and conditions of disclosure and use of information that the PCI SSC or its Members (which, for purposes of this clause, are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.) receives from the QSA either at the request and direction of Client or under PCI SSC mandatory quality assurance reviews:

a. Specifically, under Section A.6.3 – Subject Data - of the QSA Agreement, Client, upon Client's request, can authorize Trustwave to disclose each Report on Compliance ("ROC"), Attestation of Compliance and other PCI Compliance Assessment related information to the PCI SSC including employees of its Members' working for or on behalf of the PCI SSC.

b. Specifically, under Section A.10.2(b) - Audit and Financial Statements - of the QSA Agreement for purposes of complying with Trustwave's obligations and requirements related to quality assurance procedures for ensuring the reliability and accuracy of QSA Assessments, Client authorizes Trustwave to disclose the following:

   (i) Pursuant to a QSA general quality assurance review, Trustwave is authorized to disclose a copy of the Client's ROC with information redacted to include but not limited to Client's name, network diagram and other such information in an effort to limit, to the extent possible, the association of the ROC with the Client;

   (ii) Pursuant to a QSA general Disclosure Compliance Requirement review; Trustwave is authorized to provide a copy of this Agreement and any amendments to the PCI SSC including employees of its Members working for on behalf of the PCI SSC for the sole purpose of demonstrating compliance with the QSA Disclosure Readiness provisions. Sensitive information can be redacted to the extent the redacted portions do not modify or inhibit the mandatory disclosure requirements; and

   (iii) Pursuant to a QSA-specific quality assurance review in connection with a compromise of Client's systems involving cardholder data, Client authorizes Trustwave to disclose, the ROC, Attestation of Compliance, other PCI Compliance Assessment results, which includes but is not limited to work papers, notes and other relevant information, and this Agreement and any amendments to the PCI SSC including employees of its Members working for on behalf of the PCI SSC.

All disclosures will be made pursuant to Section A.6 – Confidentiality – of the QSA Agreement, and to the extent possible, Client shall be a third party beneficiary of Trustwave's QSA Confidentiality protections. Trustwave has fifteen (15) days to respond to such request, and Trustwave shall provide notice to Client of any such request, however, no additional consent, permission or approval from Client is required for Trustwave's disclosure under such request. In the event that the QSA Agreement is amended that affords Client additional protections for its Confidential Information or reduces Trustwave disclosure requirements, such protections shall be afforded to Client, or Trustwave shall agree to amend this Agreement as necessary.

2. All notices, consents, and approvals required by this Agreement may be sent by electronic mail.
3. All other terms and conditions shall remain in full force and effect.

{SIGNATURE PAGE FOLLOWS}

IN WITNESS WHEREOF, the Parties below have executed this agreement as of the date indicated below.

Trustwave: As a person authorized to enter into Agreements and contracts on behalf of Trustwave, I herby provide and accept this Agreement for the designated services and term as accepted by South Carolina Department of Revenue:

Signature: ____________________

Print Name: ____________________

Title: ____________________

Effective Date: ____________________

SOUTH CAROLINA DEPARTMENT OF REVENUE: As a person authorized to enter into agreements and contracts on behalf of South Carolina Department of Revenue, I hereby accept this Agreement for the designated services and term as initialed below:

Initial requested services and desired term

Requested Service	1- Year Term 7/01/09 thru 7/01/2010
Compliance Validation Service (CVS)	
External Penetration Test	

Signature: Terry Ellen Garber

Print Name: Terry Ellen Garber

Title: Manager, New Application Development

Date: 6-30-09

Corporate Headquarters
120 N. LaSalle Street
Chicago, IL 60602
(312) 629-1111

AmbironTrustWave
www.atwcorp.com

Addendum
To The CVS Agreement Dated March 14, 2006

PRESENTED TO:

South Carolina Department of Revenue & Tax

PREPARED BY:

PATRICK DILLON

PROPRIETARY INFORMATION

This proposal may only be used for evaluating the planned services designated herein, and may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this proposal or the information herein is prohibited without prior written permission of AmbironTrustWave.

Addendum

This is an Addendum dated September 15, 2007 to and governed by the Services Agreement ("Agreement") by and between AmbironTrustWave and South Carolina Department of Revenue and Tax dated March 14, 2006. ATW desires to provide the same Services, as identified below to Client, and Client wishes to receive such services pursuant to the terms and conditions, unless otherwise noted below, of the Agreement.

Whereas, ATW and Client mutually agree to extend the Term of the Agreement to be consistent with the Term as identified below.

Statement of Work

Compliance Validation Service

ATW shall deliver the services as described in the Agreement under the Statement of Work section for South Carolina Department of Revenue, located in Columbia, SC.

Detailed Pricing Schedule

ATW SERVICES	1 Year Term	2 Year Term	3 Year Term
Compliance Validation Service	$1,700/mo.	$1,600/mo.	$1,500/mo.

{SIGNATURE PAGE FOLLOWS}

IN WITNESS WHEREOF, the Parties below have executed this agreement as of the date indicated below.

AmbironTrustWave: As a duly elected officer authorized to enter into Agreements and contracts on behalf of AmbironTrustWave, I herby provide and accept this Agreement for the designated services and term as accepted by Client:

Signature: ______________________

Print Name: ______________________

Title: ______________________

Effective Date: ______________________

South Carolina Department of Revenue: As a duly authorized person with the authority to enter into agreements and contracts on behalf of Client, I hereby accept this Agreement for the designated services and term as initialed below, as written this 2 day of October, 2007.

Initial requested services and desired term

Requested Service	1 Year Term	2 Year Term	3 Year Term
Compliance Validation Service (CVS)	✓		

Signature: Michael D Garon

Print Name: Michael D. Garon

Title: Sr. Administrator & CIO

Date: October 2, 2007

ADDENDUM

This is an Addendum dated October 1, 2007 to and governed by the Compliance Validation Agreement ("Agreement") by AmbironTrustWave and The South Carolina Office of State Treasurer on behalf of participating governmental units ("Client"), dated September 30, 2006. ATW desires to provide additional Products and Services, as identified below to Client, and Client wishes to receive such services pursuant to the terms and conditions, unless otherwise noted below, of the Agreement.

Whereas, ATW and Client mutually agree to add to the Term of the Agreement to be consistent with the Term as identified below and the Terms and Conditions in the Statement of Work.

Statement of Work

Intrusion Prevention Managed Services (1 Monitored Networks)

IP Angel – 800 (800 Mb/s)

ATW shall deliver the product and services as described in the Agreement under the Statement of Work attached hereto.

Detailed Pricing Schedule

ATW SERVICES	1 Year Term	3 Year Term	5 Year Term
Intrusion Prevention Managed Services	$2,916/mo.	$2,770/mo.	$2,624/mo.

{SIGNATURE PAGE FOLLOWS}

IN WITNESS WHEREOF, the Parties below have executed this agreement as of the date indicated below.

AmbironTrustWave: As a duly elected officer authorized to enter into Agreements and contracts on behalf of AmbironTrustWave, I herby provide and accept this Agreement for the designated products and services and term as accepted by Client:

Signature:

Print Name:

Title:

Effective Date:

CLIENT: As a duly elected officer authorized to enter into agreements and contracts on behalf of Client, I hereby accept this Agreement for the designated services and term as initialed below:

Initial requested services and desired term

	1 Year Term	3 Year Term	5 Year Term
Intrusion Prevention Managed Services	✓		

Signature: Michael D Garon

Print Name: Michael D. Garon

Title: Sr Administrator & CIO

Date: 10/2/2007

Corporate Headquarters
120 N. LaSalle Street
Chicago, IL 60602
(877) 262-1111

AmbironTrustWave
www.atwcorp.com

Compliance Validation Service (CVS) for the Data Security Standard

Presented To:

South Carolina Office of State Treasurer

Date: June 21, 2005

Prepared By:

Molly Malone

mmalone@atwcorp.com
Phone: (410)573-6910 x7854

PROPRIETARY INFORMATION

This proposal may only be used for evaluating the planned services designated herein, and may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this proposal or the information herein is prohibited without prior written permission of AmbironTrustWave Corporation.

EXECUTIVE SUMMARY

Proposal Overview

The South Carolina Office of State Treasurer, on behalf of participating governmental units as defined in Attachment A, has Level 2, 3 and 4 Merchants as defined by the Payment Card Industry Data Security Standard (PCI) that are seeking to validate their compliance. AmbironTrustWave (ATW) is authorized to perform the following Compliance Validation Services (CVS) to assess and validate compliance and help you maintain compliance throughout the term of this agreement:

- **Compliance Validation Service (CVS):**
  - Remote Validation Service
  - Vulnerability Scanning Service
  - Support
- **Optional services are available from ATW to address the below PCI requirements:**
  - Network Penetration Testing (PCI Requirement 11)
  - Policy and Procedure Development (PCI Requirement 12)
  - Building a Secure Network (PCI Requirements 1 and 2)
  - Implement Strong Access Control Measures (PCI Requirements 7, 8 and 9)
  - Regularly monitoring and testing networks (PCI Requirements 10 and 11)

AmbironTrustWave Overview

ATW is the leading provider of data security and compliance services to all businesses in the payment industry including acquirers, service providers, third-party providers, and merchants. ATW is headquartered in Chicago, Illinois and has 12 offices throughout North America. A summary of our payment industry credentials and information security experience is outlined below:

- **Leading Assessor** - ATW has performed more than 300 Level 1 and Level 2 assessments for Merchants and Service Providers since the Visa CISP program was launched in June 2001. ATW is the only company authorized by all of the major card associations (American Express, Discover, MasterCard and Visa) to validate compliance, scan merchants, and provide computer forensic services. To date, all of Visa's Payment Application Best Practices (PABP) compliant application vendors were validated by ATW's ***TrustedApp®*** service.
- **Innovative Solutions** - ATW's enterprise compliance suite, ***TrustKeeper®***, has been approved by all of the card associations to validate PCI compliance and is endorsed by over 30 Merchant Acquiring Banks. TrustKeeper currently supports over 25,000 merchants in their efforts to achieve and maintain compliance. TrustKeeper is accessible through a secure easy-to-use portal backed by a multi-lingual 12x5 (12 hrs a day, five days a week) help desk. TrustKeeper can also be leveraged to validate compliance against HIPAA, GLBA, SOX, FISMA and ISO17799.
- **Data Security Experts** - For more than 10 years ATW professionals have been delivering information technology solutions to the Fortune 1000 and government agencies. ATW's ***TrustSentry®*** suite offers customers a comprehensive array of managed security services including intrusion detection, firewall management or monitoring, VPN, anti-virus, authentication, and vulnerability scanning. The TrustSentry management console provides integrated trouble-ticketing, online help, and real-time reporting.

SERVICES AGREEMENT

This Compliance Validation Services Agreement ("Agreement"), is made by and between AmbironTrustWave, operating under TrustWave Holdings, Inc, a Delaware Corporation ("ATW") and the South Carolina Office of State Treasurer, on behalf of participating governmental units as defined in Attachment A,("Client"), and shall be effective as of the date of execution by both parties. ATW desires to provide Compliance Validation Services to Client to address the Payment Card Industry (PCI) Data Security Standard and other major card association security requirements as described in this Agreement, and Client wishes to receive such services.

Statement of Work

Compliance Validation Service (CVS)

ATW will provide Client with a Compliance Validation Service designed to manage the overall compliance process and aid in achieving the compliance objectives. An ATW consultant will host weekly calls throughout a two-month period after the initial questionnaire and scan are completed. The purpose of the calls will be to identify areas of non-compliance uncovered in the questionnaire and scan results, develop and assist in managing a remediation plan to address the non-compliance issues, validate policies and procedures, and review network security infrastructure and architecture. Based on our extensive experience and knowledge, typical areas of non-compliance include card data encryption, multi-factor authentication, and system logging. The Compliance Validation Service consists of:

1. **Remote Validation Service.**
   a. **Online Questionnaire:** PCI requires that all merchants and service providers complete the PCI self-assessment questionnaire. The TrustKeeper system provides an easy to use portal that satisfies the requirements of all the card associations with self-help and a continuously updated FAQ database. The questionnaire is available in English and French.
   b. **Documentation of Results:** At the conclusion of the assessment, a Compliance Validation Report will be created detailing the findings from the Compliance Validation Service which will include the identification of any non-compliance issues. The report will also provide a remediation plan with recommendations for non-compliance issues..
2. **Vulnerability Scanning Service.**
   a. **Scanning:** The automated vulnerability scanning engine within TrustKeeper is a proprietary "Intelligent" scanning solution that has been tested and determined to be PCI compliant. The scanning solution tests for more than 3,000 unique vulnerabilities and is extremely accurate in eliminating false positives. You are entitled to receive monthly scans during the term of the Agreement for up to (**512**) IP addresses.
   b. **Reporting:** Through a secure web interface, TrustKeeper provides easy access to concise, auto-generated reports with a high-level summary for executives and managers. The reports will also provide detailed results and remediation action for technicians. Remediation instructions include CVE-linked vulnerability checks and best practices defined by ATW consultants.
   c. **Security:** ATW's TrustKeeper infrastructure is monitored on a 24x7 basis to ensure protection of Client data. All Client data is delivered via secure channels.
3. **Support.**
   a. ATW provides comprehensive online support through the TrustKeeper portal that includes self-help and a continuously updated FAQ database. In addition, email and multilingual phone support are available during standard business hours to answer any questions regarding PCI compliance or vulnerability scanning results.

Optional Remediation Services

ATW offers a full suite of Remediation Services to help you achieve and maintain compliance. The following services may be included as optional services:

Network Penetration Service (NPS)

PCI requirement 11 and Guideline 2 of Discover DISC require that penetration tests are conducted at least annually or after any significant change to your network. This service is designed to satisfy these requirements and includes the following:

1. **Enumeration**: A list of targeted and authorized IP addresses will be developed based on Client provided data (domain names, network blocks and individual IP addresses). This includes intelligent domain name resolution in which dynamic, periodic name resolution is employed in order to discover load-balancing architectures that utilize multiple public IP addresses.
2. **Inventory**: ATW determines which of the enumerated IP addresses are actually running, available and offering network services. Host inventory uses a number of techniques, including ICMP pings, common TCP service probes, and protocol-specific UDP service probes. In local, LAN-based scans, ARP queries also reveal active systems. Open services are probed for any information that can be used to verify the actual application layer protocol (e.g., HTTP), as well as vendor applications (e.g. Apache, IIS, Netscape, Domino) and version.
3. **System_Discovery**: ATW attempts to identify other IP addresses associated with the target IP addresses. Typical discovery methods include DNS record lockups and various dynamic port-mapping techniques (e.g., DCE Endpoint Mapping and Java RMI Registry probes). Although no active scans are performed on "discovered" devices, this information can reveal additional "reconnaissance" information about a network. Clients should, if they own or are authorized to, add these associated IP addresses to their scan profile for their next scan.
4. **Vulnerability Checks:** ATW performs specific checks for vulnerabilities on all accessible host IP addresses and services using a variety of proprietary and commercial tools. These tools minimize network traffic by applying their tests in an intelligent manner (e.g., Apache server is not tested for IIS specific vulnerabilities).
5. **Manual Analysis and Verification**: ATW will conduct a manual verification and analysis of the discovered vulnerabilities on Internet facing systems to identify security holes and eliminate false positives. ATW analyzes the discovered vulnerabilities in the context of the overall system architecture and identifies conditions that would allow lower severity vulnerabilities to be used together for system exploitation.

The service will be performed on up to (**2**) devices. Upon completion of the testing, a report will be provided documenting the findings and include high-level recommendations to assist you in correcting any areas of deficiency. All testing phases will be coordinated with Client to minimize any adverse impact that may occur as a result of the services. We strongly recommend full-disclosure of the testing to all individuals responsible for the network and related services and devices. Although we take precautions to minimize the negative impact on client systems, we do not guarantee against service interruptions due the inherent risk of such testing that could result from unpatched systems, unique system configurations, and other such issues. We also recommend the establishment of incident response procedures in the event of any adverse impact or disruption of network services. Client assumes full responsibility to backup and/or otherwise protect its data against loss, damage or destruction prior to and during all phases of the proposed services, and to take appropriate measures to respond to any adverse impact of the systems or disruption of service.

Policy & Procedure Service (PPS)

PCI requirement 12 requires that companies develop, implement, and enforce an Information Security Policy. ATW will provide you with consulting services to assist in the development of Information Security Policy and Procedures that address the relevant card association requirements. The documents will be created in conjunction with the South Carolina Office of State Treasurer, on behalf of participating governmental units, and your IT staff to ensure that it reflects the specific environment and procedures of your operating environment. The PCI required policy and procedures, and our consulting process are detailed below:

- Backups
- Change Control
- Data Control
- Data Retention
- Disaster Recovery
- File Integrity
- Firewall Administration
- Media Maintenance
- Incident Response Plan
- ID and Password
- Key Management and Storage
- Periodic Operational Testing
- Physical
- System Hardening
- Vulnerability Management

ATW's consulting process consists of:

1. **Data Gathering:** ATW's security consultants will conduct a series of in-depth interviews in order to gain an understanding of your business' operating environment. This information will be gathered during weekly calls and serve as the framework of the policy and procedure documents. Your staff will provide ATW with the current set of internal procedural steps.
2. **Draft Creation:** Subsequent to the data gathering phase, ATW will create a comprehensive set of policies and procedures that will address the needs of your company and help you achieve PCI compliance.
3. **Review & Modification:** ATW will then review the draft with your staff to ensure that all of security and compliance objectives are addressed. Any necessary additions or modifications will be made to the draft at this time.
4. **Delivery & Implementation:** Once the policies and procedures meet your approval, ATW will deliver a final version for your implementation. ATW can, if necessary, assist you with the implementation phase by providing consulting serivces at a reduced and cost effective rate.

In the event that additional consulting services are required, the parties will agree to any additional efforts and fees, in writing, prior to the initiation of the additional services. If the multi-year service is selected, the service includes updating the existing policies to include new policies or changes as required by the card associations.

Subsequent years of Agreement will utilize the same methodology and request Client to identify changes within the environment. These changes may require the adjustment of existing policies and procedures. This can include technological changes such as newly deployed systems or devices, system configuration changes, firewall policy changes as well as adjustments to roles, responsibilities and internal processes. Additionally, these documents will be updated to include new PCI requirements as required by the card associations.

PRICING

Detailed Pricing Schedule

ATW Service	Level	Monthly Credit Card Dollar Volume	1-Year Term
Standard Service - Includes On-Line Questionnaire and Vulnerabilty Scan	1	>$1 million	$199.50/mo.
Standard Service - Includes On-Line Questionnaire and Vulnerability Scan	2	>$250,000	$129.50/mo.
Standard Service - Includes On-Line Questionnaire and Vulnerability Scan	3a	>$50,000	$37.44/mo.

ATW Service	1-Year Term	3-Year Term	5-Year Term
Compliance Validation Service (CVS) - Includes Standard Service	$625/mo.	$525/mo.	$525/mo.
Network Penetration Service (NPS)	$125/mo.	$105/mo.	$95/mo.
Policy & Procedure Service (PPS)	$750/mo.	$350/mo.	$266/mo.

1. Travel and expenses are not included in the fees and will be billed separately. ATW will use commercially reasonable efforts to travel as efficiently and cost effective as possible given timing and travel requirements. Valid expenses typically include parking, meals, lodging, photocopying, communication costs, airfare, mileage, and/or automobile rental.
2. Participating governmental units shall process payment to ATW within thirty (30) work days. The thirty (30) work days begins after the governmental unit certifies its satisfaction with the receipt of services and proper invoice. Governmental units shall pay an amount not to exceed fifteen percent per annum on any unpaid balance which exceeds the thirty (30) work day period as pursuant to the SC Code of Laws.
3. Proposals are valid for up to sixty days from the date on the cover page.

Project Deliverables

Submission of the final deliverable constitutes the end of the project. A deliverable shall be deemed accepted if not rejected by Client, in writing, within five business days of receipt.

Deliverable	Description	Completion Date
Vulnerability Scan Report	Up to one vulnerability scan per month during the term will be conducted with a report delivered via the TrustKeeper portal. The report will incorporate both questionnaire and scan results.	Upon completion of questionnaire and vulnerability scan

Compliance Validation Report	A report detailing the findings from the Compliance Validation Service which will include the identification of any non-compliance issues. The report will also provide a remediation plan with recommendations for non-compliance issues.	TBD
Statement of Compliance	Upon achieving PCI Compliance, Client will be provided with a Statement of Compliance letter.	Upon achieving compliance
Penetration Test Report	A report detailing the findings of the manual verification and analysis of discovered vulnerabilities.	Optional Service
Policy and Procedures Documents	As a result of the Procedures Services, ATW will develop a set of Information Security Procedures addressing the PCI Data Security Standard.	Optional Service

PREREQUISITES

Dependencies and Assumptions

This Agreement was developed based on the following dependencies and assumptions, which if not accurate or adhered to, may require a change in the scope of services. Any change in services and fees will be mutually agreed to in writing by both parties. The dependencies and assumptions include:

1. ATW shall not begin to provide the Services as described in this Statement of Work (SOW) until Client has returned this signed SOW and a Purchase Order (PO) for the total amount of the Services selected (full contract amount).
2. Client's Primary Contact (PC), as identified below or their designee must be available to ATW during the entire engagement. The representative must have sufficient authority to schedule testing and address any issues that may arise.
3. Client will provide ATW with sufficient information to evaluate compliance for all PCI requirements. Client is solely responsible for providing access to and coordinating any required interviews or testing with Client's third parties or service providers.
4. If needed, Client will provide resources and information as requested to enable ATW's consultants to sufficiently develop documentation consistent with PCI Information Security Policy requirements. This will include access to personnel who can provide information related to the business operations, organizational structure, network architecture, security controls, disaster recovery and general daily operational processes and procedures.
5. During testing, the configuration of Client's network will be kept as stable as possible (i.e., no new systems or configuration changes). If changes are required, then Client shall inform ATW, and a mutually acceptable testing schedule shall be agreed upon..

Contact Information

Contact	State of South Carolina State Treasurer's Office
Name:	Karen Wicker
Title:	Senior Assistant State Treasurer, Administration Division
Phone/Fax:	803-734-9871/803-734-2690
E-mail Address:	wickk@sto.state.sc.us
Billing Address:	PO Box 11778 Columbia, SC 29211
Assessment Site Address (if different):	______________________________

TERMS AND CONDITIONS

1. **IP Addresses, URL and Domain Names**. South Carolina Office of State Treasurer, on behalf of participating governmental units, represents and warrants that the South Carolina Office of State Treasurer, on behalf of participating governmental units, has full right, power and authority to consent to have the TrustKeeper service scan for vulnerabilities the IP address and/or URL and/or domain names identified to AmbironTrustWave (ATW) by Client for scanning, whether electronically or by any other means, whether during initial enrollment or thereafter. South Carolina Office of State Treasurer, on behalf of participating governmental units, shall be liable, to the full extent permitted by State of South Carolina state law and regulations, for any and all claims for wrongful death, personal injury, or property damage incurred by reason of negligence of the South Carolina Office of State Treasurer, or its employees and arising from activities under this Section 1.. Client acknowledges and understands that accessing and scanning IP addresses and penetration testing involves inherent risks, including, without limitation, risks related to system or network performance and availability, and data corruption or loss.

2. **Applicable Laws and Restrictions**. South Carolina Office of State Treasurer's use, on behalf of participating governmental units, of the TrustKeeper portal, reports, and scanning solution is subject to the following restrictions: (a) South Carolina Office of State Treasurer, on behalf of participating governmental units,, may use the TrustKeeper services and portal only to scan IP addresses, URLs and domain names owned by and registered to South Carolina Office of State Treasurer, on behalf of participating governmental units,; (b) the TrustKeeper services, portal and reports may only be used for the stated purposes in this Agreement for South Carolina Office of State Treasurer's internal business purposes, on behalf of participating governmental units, in accordance with all applicable laws (including any export control laws); and, (c) Client shall limit access to the TrustKeeper portal to only those employees and/or contractors who have executed a written confidentiality agreement with Client and only to those who have a requirement for such access on a "need to know" basis.

3. **Warranty.** ATW warrants to South Carolina Office of State Treasurer, on behalf of participating governmental units, that all Services shall be performed by employees or contractors of ATW in a professional and workmanlike manner. Each party warrants that (i) it has the full right and power to conduct its business; (ii) that this Agreement has been duly authorized, executed and delivered, and constitutes a valid and binding Agreement in accordance with the terms herein; and (iii) neither the execution or consummation of the services contemplated shall result in the breach or default of any other agreement, charter provision or bylaw, order, law, rule or regulation.

4. **LIMITATION OF LIABILITY AND DISCLAIMER OF WARRANTY.**

   a. ATW SHALL NOT BE LIABLE TO SOUTH CAROLINA OFFICE OF STATE TREASURER, ON BEHALF OF PARTICIPATING GOVERNMENTAL UNITS, FOR (1) ANY ACTS OR OMISSIONS WHICH ARE NOT THE RESULT OF ATW'S GROSS NEGLIGENCE, RECKLESSNESS OR WILLFUL MISCONDUCT, (2) ANY AMOUNTS IN EXCESS OF ANY FEES PAID TO ATW BY CLIENT HEREUNDER, (3) ANY OUTAGES OR SLOW DOWNS OF SOUTH CAROLINA OFFICE OF STATE TREASURER'S, ON BEHALF OF PARTICIPATING GOVERNMENTAL UNITS, COMPUTER SYSTEMS RESULTING FROM THE PERFORMANCE OF ANY SERVICES, UNLESS SUCH OUTAGES OR SLOW DOWNS ARE THE RESULT OF ATW'S GROSS NEGLIGENCE, RECKLESSNESS OR WILLFUL MISCONDUCT, OR (4) ANY LOSSES, COSTS, DAMAGES OR EXPENSES INCURRED BY CLIENT RESULTING FROM THE PERFORMANCE OF ANY TEST, UNLESS SUCH ARE THE RESULT OF ATW'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

   b. THIS AGREEMENT IS A SERVICE AGREEMENT, AND EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, ATW DISCLAIMS ALL OTHER REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES REGARDING QUALITY, SUITABILITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE (IRRESPECTIVE OF ANY COURSE OF DEALING, CUSTOM OR USAGE OF TRADE) OF ANY SERVICES OR ANY GOODS OR SERVICES PROVIDED INCIDENTAL TO THE SERVICES PROVIDED UNDER THIS AGREEMENT.

   c. IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY SPECIAL, INDIRECT, EXEMPLARY, INCIDENTAL, OR CONSEQUENTIAL LOSSES OR DAMAGES, INCLUDING LOST PROFITS WHETHER FORESEEABLE OR NOT, WHETHER OCCASIONED BY ANY FAILURE TO PERFORM OR THE BREACH OF ANY REPRESENTATION, WARRANTY, COVENANT OR OTHER OBLIGATION FOR ANY CAUSE WHATSOEVER.

5. **Proprietary Rights.** South Carolina Office of State Treasurer, on behalf of participating governmental units, acknowledges and agrees that, as between ATW and South Carolina Office of State Treasurer, on behalf of participating governmental units, all right, title and interest in and to the TrustKeeper portal and its contents, the TrustKeeper Scanning Solution and any part thereof, including, without limitation, all patents, copyrights, trade secrets and all other intellectual property rights therein and thereto, and all copies thereof, in whatever form, including any written documentation shall at all times be and remain solely with ATW. South Carolina Office of State Treasurer, on behalf of participating governmental units, shall not be an owner or licensee of the TrustKeeper portal and related software.

6. **Term.** This Agreement shall be for a term of one year (Initial Term) commencing on the date of execution by both parties, and subject to earlier termination as provided in this Agreement. Following the Initial Term, this Agreement shall automatically renew, with such amendments as to which the parties shall agree, for additional one (1) year periods unless either party provides written notice to the other party, at least ninety (90) days prior to the conclusion of the then-current term, of its intention not to renew.

7. **Termination for Cause.** Either party may terminate this Agreement for cause (a) upon the expiration of thirty (30) calendar days following detailed written notice to the other party of its material breach of any of its material obligations under this Agreement, provided that the other party has not remedied such breach during the notice period, or (b) immediately upon written notice to the other party if a petition in bankruptcy is filed by or against the other party and is not withdrawn within 60 days or the other party makes an assignment for the benefit of its creditors or an arrangement pursuant to any bankruptcy law, or if the other party discontinues its business or a receiver is appointed for its business.

8. **Effect of Termination; Survival.** If a participating governmental unit terminates this Agreement for any reason, the participating governmental unit agrees to pay ATW within 30 days for all services performed by ATW up to the date of cancellation that have not previously been paid for by the participating governmental unit. Additionally, if Client terminates this Agreement other than for cause, then the participating governmental unit shall pay to ATW, as a cancellation fee and not as a penalty, an amount equal to the sum of the monthly service charges for the remainder of this agreement. The provisions of this section 9, sections 1, 2, 4, 5, 6, 11, 17, 20 and 21 shall survive any expiration or termination of this Agreement.

9. **Payment Card Association Compliance.** You acknowledge and agree that your use of the services does not guarantee PCI compliance or that your systems are secure from unauthorized access. You are responsible for PCI compliance and notification of any suspected breach of your systems. You are solely responsible for any fines, penalties or registration fee imposed by any payment card association and your Acquirer.

10. **Confidentiality and Authorized Disclosure.** ATW and South Carolina Office of State Treasurer, on behalf of participating governmental units, hereby confirm that the provisions of a mutual non-disclosure agreement between ATW and South Carolina Office of State Treasurer, on behalf of participating governmental units,, if executed, shall be in full force and effect and apply to all information furnished by either party in connection the services. In addition, Client authorizes ATW to release all Client reports to the Client's merchant acquiring bank, if applicable, and the payment card association for reporting PCI compliance.

11. **Dependencies.** Client acknowledges that the provision of services is dependent upon the performance of Client, and its affiliates, and that ATW shall not be liable for its failure to perform to the extent such failure is due to (i) a failure by Client or any third party retained by, or under the control of, Client to provide data or materials that Client or such third party is required to provide to ATW or required by ATW to perform the services under this Agreement, (ii) a failure by Client to timely and accurately perform its responsibilities as set forth in this Agreement, or (iii) a failure by Client to obtain consents, approvals or access for ATW.

12. **Force Majeure.** Neither party shall be liable for any default or delay in the performance of its obligations hereunder (except for payments) if and to the extent such default or delay is caused, directly or indirectly, by acts of God, governmental acts, accidents, wars, terrorism, riots or civil unrest, fires, storms, earthquakes, floods or elements of nature, or any other similar cause beyond the reasonable control of such party, provided such default or delay could not have been prevented by reasonable precautions and cannot reasonably be circumvented by the non-performing party through the use of commercially reasonable alternative sources, workaround plans or other means.

13. **Entire Agreement and Amendments.** This Agreement, together with an executed mutual non-disclosure agreement, if any, constitutes the entire Agreement among the parties pertaining to the subject matter hereof and supersedes all prior and contemporaneous, oral and written, agreements and understandings pertaining thereto. Any amendment to this Agreement must be in writing, mutually agreed upon and duly executed. The waiver or failure of either party to exercise any right provided for in this Agreement shall not be deemed a waiver of any further or future right under this Agreement.

14. **Assignment.** Neither party may assign, delegate nor otherwise transfer the rights or obligations associated with this Agreement, in whole or in part, without the prior written consent of the other party; provided however, no written consent shall be required to assign this Agreement to any parent or the wholly owned subsidiary of the party. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties, their respective successors and permitted assigns.

15. **Counterparts.** This Agreement may be executed in two or more counterparts, each of which when so executed will be deemed original, and all of which together will constitute one and the same instrument.

16. **Trademarks and Logo.** Client shall not have any rights to use ATW's trademarks, service marks or logos for any other purpose without the prior written approval of ATW's legal department.

17. **Severability.** Any term or provision of this Agreement that is or becomes invalid or unenforceable shall be Ineffective to the extent of such invalidity or unenforceability without rendering invalid or unenforceable the remaining terms or provisions of this Agreement.

18. **Limitation.** All obligations are limited by and subject to the laws of the State of South Carolina.

19. **Advertising.** ATW agrees not to refer to this Agreement in commercial advertising in such a manner as to state or imply that ATW is endorsed or preferred by the State Treasurer, the State of South Carolina, or any unit of either.

20. **Limited Statutory Walver of Sovereign Immunity.** Title 11, Chapter 35, Article 17 constitutes a limited statutory waiver of sovereign immunity. ATW agrees that no act by either the State Treasurer or any unit of South Carolina government regarding this Agreement or any transaction contemplated herein is a waiver of either their sovereign immunity or their immunity under the Eleventh Amendment of the United State's Constitution. Both the rights and obligations of the parties, this Agreement and any transaction contemplated by this Agreement, as well as any related dispute, claim, or controversy, shall, in all respects, be established, interpreted, construed, enforced and governed by and under the laws of the State of South Carolina, without regard to any provision governing conflicts of law. All disputes, claims, or controversies arising out of or in any way relating to this Agreement or any transaction contemplated by this Agreement shall be resolved exclusively by the appropriate Chief Procurement Officer in accordance with Title 11, Chapter 35, Article 17 of the South Carolina Code of Laws, or in the absence of jurisdiction, only in the Court of Common Pleas for Richland County, State of South Carolina.

21. **Third-Party Beneficiaries.** Nothing herein expressed or implied is intended to or shall be construed to confer upon or give any person or entity, other than the parties hereto and their respective successors and permitted assigns, any rights or remedies under or by reason of this Agreement.

22. **Non-Solicitation.** During the term and for a period of one (1) year thereafter, South Carolina Office of State Treasurer, on behalf of participating governmental units, shall not, directly or indirectly solicit, hire, attempt to solicit or hire, or participate in any attempt to solicit or hire any person who was an employee of ATW or any of its Affiliates.

23. **Relationship of Participating Governmental Units.** Each participating governmental unit's obligations and liabilities are Independent of every other participating governmental unit's obligations and liabilities. No participating governmental unit shall be responsible for any other participating governmental unit's act or failure to act. Any contracts awarded as a result of this procurement are between ATW and the participating governmental units. The State Treasurer's Office is not a party to such contracts, unless and to the extent that the State Treasurer's Office is a participating governmental unit, and bears no liability for any party's losses arising out of or relating in any way to the contract.

24. **Notice.** Except as otherwise provided in this Agreement, all notices, consents, or approvals required by this Agreement shall be (i) in writing sent by certified or registered mail, postage prepaid, or by facsimile or electronic mail (confirmed by certified or registered mail) to:

AmbironTrustWave
c/o TrustWave Holdings, Inc.
PO Box 4815, Annapolis. MD 21403
Attention: Legal Department
Fax: (410) 571-8493

South Carolina Office of State Treasurer:
on behalf of participating governmental units
PO Box 11778, Columbia, SC 29201
ATTN: Karen Wicker, Administrative Division
Fax: (803) 734-2690

or (ii) in any other manner mutually agreed upon by the Parties. Notices shall be deemed effective on the date of mailings.

{SIGNATURE PAGE FOLLOWS}

SIGNATURES

IN WITNESS WHEREOF, the Parties below have executed this agreement as of the date indicated below.

AmbironTrustWave: As a duly elected officer authorized to enter into Agreements and contracts on behalf of AmbironTrustWave, I herby provide and accept this Agreement for the designated services and term as accepted by Client, as written this day this 30 day of Sept, 2005.

Signature: ____________________

Print Name: Phillip Smith

Title: EVP

Effective Date: 9/30/05

South Carolina Office of State Treasurer, on behalf of participating governmental units: As a duly elected officer authorized to enter into agreements and contracts on behalf of Client, I hereby accept this Agreement for the designated services and term as initialed below, as written this ____ day of ____________, 2005.

Initial requested services and desired term (please check all that apply):

ATW Service	Level	Monthly Dollar Volume	1-Year Term
Standard Service - Includes On-Line Questionnaire and Vulnerability Scan	1	>$1 million	
Standard Service - Includes On-Line Questionnaire and Vulnerability Scan	2	>$250,000	
Standard Service - Includes On-Line Questionnaire and Vulnerability Scan	3a	>$50,000	

Requested Service	1 Year Term	3 Year Term	5 Year Term
Compliance Validation Service (CVS)			
Network Penetration Service (NPS)			
Policy & Procedure Service (PPS)			

Signature: Grady L Patterson

Print Name: Grady L. Patterson, Jr.

Titie: State Treasurer

Date: September 30, 2005

ATTACHMENT A

For the purpose of this service agreement, the term "participating governmental unit" is defined as any State of South Carolina agency or Institution which meets the following criteria: a) have a current participation agreement for credit card services under the State Treasurer's Office Merchant Services Bankcard Agreement; b) have signed a current participation agreement for compliance validation services under the State Treasurer's Office Compliance Validation Services Agreement; and c) have submitted a purchase order to ATW for services pursuant to the agreement.

Issue C-108 to:

Trustwave Holdings, Inc.
120 N. Lasalle St
Suite 1250
Chicago, IL 60602

Contract #: Per Contract with State Treasurer's Office

Line	UOM	Description	Each	Total
1	LOT	PCI Validation Service to include -Compliance Validation Service -Network Penetration Service -Policy & Procedure Service @ $1700 a month	$20400.00	$20400.00
2	LOT	IP Angel 800 Intrusion Prevention Managed Services @ $2916 a month	$34992.00	$34992.00
			Total:	$55392.00