FOURTH AMENDATORY AGREEMENT

FOURTH AMENDATORY AGREEMENT is made and entered into by and between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the "City"), and **TRUSTWAVE HOLDINGS, INC.**, a Delaware corporation doing business at 70 W. Madison Street, Suite 1050, Chicago, IL 60602 (the "Consultant") collectively (the "Parties").

WITNESSETH:

WHEREAS, the Parties entered into an Agreement dated October 23, 2007 and amended the Agreement on November 24, 2009, December 14, 2010 and on May 25, 2011(the "Agreement"), relating to validation of the City's compliance against the Payment Card Industry Data Security Standards and continued ongoing compliance, and

WHEREAS, the Parties wish to amend the Agreement to update the scope of work, extend the term, increase the compensation to the Consultant; and

NOW, THEREFORE, in consideration of the premises and the mutual covenants and obligations herein set forth, the Parties agree as follows:

1. All references to "…Exhibit A and A-1…" in the existing Agreement shall be amended to read: "…Exhibit A, A-1 and A-2, as applicable…". The scope of work marked as Exhibit A-2 is attached and incorporated by reference.

2. That Article 3 of the Agreement entitled "**TERM**" is amended to read as follows.

> "**3**. **TERM**: The Agreement will commence on September 1, 2007 and will expire on December 31, 2013 (the "Term"). Upon the written instruction of the Manager, and notice to the City Controller, this Agreement may be extended for an additional one year term upon the same terms and conditions contained herein."

3. That Articles 4(a) and 4(d)(1) entitled "**Fee**" and "**Maximum Contract Amount**" are amended to read as follows:

> "**4**. **COMPENSATION AND PAYMENT**:
>
> **a**. **Fee**: The Consultant's sole compensation for its services rendered and costs incurred under the Agreement is not to exceed **Seven Hundred Ninety Eight Thousand Dollars ($798,000.00)** and amounts billed may not exceed the rates set forth in Exhibits A, A-1 and A-2, Detailed Pricing Schedule.

d. Maximum Contract Amount:

(1) Notwithstanding any other provisions of the Agreement, the City's maximum payment obligation will not exceed **Seven Hundred Ninety Eight Thousand Dollars ($798,000.00)** (the "Maximum Contract Amount"). The City is not obligated to execute an Agreement or any amendments for any further services, including any services performed by Consultant beyond that specifically described in Exhibit A, A-1 and A-2. Any services performed beyond those set forth therein are performed at Consultant's risk and without authorization under the Agreement. The Manager may modify the SOW, with the consent of the Consultant, by written authorization provided no additional funds are required."

4. The Parties agree to delete clause 42(a) of the Agreement dated October 23, 2007 and replace it with the following:

"**42(a)** Consultant shall not be liable to the City for **(1)** any acts or omissions which are not the result of Consultant's negligence, recklessness or willful misconduct, **(2)** any amounts in excess of one and half times the fees paid to Consultant by the City hereunder, **(3)** any outages or slow downs of the City's computer systems resulting from the performance of any services, unless such outages or slow downs are the result of Consultant's negligence, recklessness or willful misconduct, or **(4)** any losses, costs, damages or expenses incurred by the City resulting from the performance of any test, unless such are the result of Consultant's negligence or willful misconduct. Section 42(a)(2) herein shall not limit Consultant's liability for its indemnification obligation to the City **(i)** for Consultant's breach of its confidentiality obligation to the City and **(ii)** for Consultant's infringement of a third party's intellectual property rights. Consultant's indemnification obligations hereunder, other than those listed in the preceding sentence shall be limited to one million dollars ($1,000,000)."

5. This Amendatory Agreement may be executed in two (2) counterparts, each of which shall be deemed to be an original, and all of which, taken together, shall constitute one and the same instrument.

6. Except as herein amended, the Agreement affirmed and ratified in each and every particular.

EXHIBIT LIST:

EXHIBIT A-2 – SCOPE OF WORK

[SIGNATURE PAGES FOLLOW]

Addition to the Statement of Work dated October 23, 2007

Presented To:

City and County of Denver

February 17, 2012

Prepared By:

Hugh Jones
HJones@trustwave.com
303-679-1434

Formatted: Font: 9 pt

Formatted: Left

ADDITION

This is an Addition, dated as of the date executed below, to and governed by the Statement of Work ("Agreement"), by and between Trustwave Holdings, Inc. ("Trustwave") and City and County of Denver ("Client"), dated October 23, 2007. 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 of Addition

The purpose of this Addition is to add the services listed below.

Service Start Date

The services under this Addition shall commence as of January 31, 2012 and will end on January 31, 2013.

Formatted: Font: 9 pt

Formatted: Left

~~Statement of Work~~

Formatted: Centered, Space Before: 0 pt

Compliance Validation Service (CVS)

Trustwave will provide City and County of Denver 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 City and County of Denver throughout the CVS process, to support internal efforts to gain compliance. This includes:

- **Remediation Guidance**: A Trustwave consultant will host a series of weekly calls 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.

CVS consists of five phases, and to ensure comprehensive and efficient service, City and County of Denver must fulfill its obligations within each phase before progressing to subsequent phases. Failure to do so may require an addition 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 City and County of Denver wishes to receive any remediation services, City and County of Denver must specifically select those services.

Project Phases and Chronology

Phase I: 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 City and County of Denver 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. City and County of Denver is entitled to receive monthly scans during the term of the Agreement for up to (**256**) IP addresses.

Formatted: Font: 9 pt

Formatted: Left

Phase II: Remote Validation Service

Document and Evidence Collection

PCI requires documentation and evidence to be collected during the assessment process. Documentation includes, but is not limited to, security policies and procedures, configuration documents, and network diagrams. During this stage, Trustwave will schedule weekly calls to collect the necessary documentation. Trustwave uses a proprietary tool to collect and assist in the task of collecting required documentation and evidence. Conferences will be scheduled for one hour, but may vary based upon the needs of City and County of Denver and Trustwave.

Document and Evidence Analysis

Trustwave will review and analyze all submitted documentation to include all policies, procedural documents, standards, system configurations and other evidence as required for validating PCI compliance. In addition, any areas of non-compliance will be identified, documented and reported to City and County of Denver for appropriate action.

Phase III: 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 City and County of Denver. 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 City and County of Denver 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.

Formatted: Font: 9 pt

Formatted: Left

4. **System Vulnerability Exploitation:** If the plan of attack devised in the previous step includes any techniques that may impact production systems and infrastructure, City and County of Denver is first advised of the possible system downtime that may arise. At this point it is up to City and County of Denver 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 City and County of Denver 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 City and County of Denver'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 City and County of Denver's key security contacts on the applications identified, and what will be tested. If the system is a production system, City and County of Denver 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, City and County of Denver's key security contacts will be notified. At that time, City and County of Denver 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

Formatted: Font: 9 pt

Formatted: Left

similar to those used to develop the network map and system classification, SpiderLabs will launch a new stage of discovery against the environment.

External Penetration Test

PCI DSS requirement 11.3 states that penetration tests must be conducted at least annually or after any significant change to the City and County of Denver network. The testing will not help satisfy the PCI DSS requirement if (i) any step outlined herein is not permitted and successfully completed, (ii) the Trustwave testing methodology is not strictly followed, or (ii) Client adds restrictions on the testing. This service is performed as a non-credentialed test, and includes the following:

Trustwave will perform External Penetration Test service on the following environment:

Number of externally facing Class C networks:	**2**
IP's & IP Ranges **Description**	
169.133.255.4 primary public DNS	
169.133.255.5 secondary public DNS	
169.133.245.0/24 DMZ-Payment Gateway	
Number of remote access devices	**2**
Number of Web servers with dynamic content	**4**

Upon completion of the testing, a report documenting the findings and high-level recommendations to assist City and County of Denver in correcting any areas of deficiency will be provided. All testing phases will be coordinated with City and County of Denver to minimize any adverse impact that may occur as a result of the services. Trustwave strongly recommends full-disclosure of the testing to all individuals responsible for the network and related services and devices. Although Trustwave takes precautions to minimize the negative impact on City and County of Denver systems, Trustwave does not guarantee against service interruptions due to the inherent risk of such testing that could result from unpatched systems, unique system configurations and other such issues. Trustwave also recommends establishing incident response procedures in the event of any adverse impact or disruption of network services. City and County of Denver 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.

Internal Penetration Test Service

The PCI DSS requirement 11.3 for internal penetration testing includes any internal network and system that stores, processes or transmits cardholder data. The objective of an internal network

Formatted: Font: 9 pt

Formatted: Left

penetration test is to determine if the current network security controls are vulnerable to an actionable attack from an attacker that has gained access to the network either physically or virtually. This level of testing validates corporate security policy and development standards by attempting to identify how resilient the internal network is to determined attackers. The product of an internal network penetration test is a report that documents the organization's existing security posture, identifies specific weaknesses and vulnerabilities, and provides purpose built exploit code examples that tell a compelling story of risk from any given vulnerability, and makes recommendations for their remediation. The testing will not help satisfy the PCI DSS requirement if (i) any step outlined herein is not permitted and successfully completed, (ii) the Trustwave testing methodology is not strictly followed, or (ii) Client adds restrictions on the testing.

Remote Internal Test Option

Remote internal testing is accomplished via a Trustwave-provided hardware-based remote penetration testing (RPT) appliance, or a software-based virtual remote penetration testing (VRPT) appliance to facilitate remote access. Trustwave retains all right, title and interest to such hardware. A comparison of the two appliance testing options is included below:

Remote Penetration Test (RPT)Appliance	**Virtual Remote Penetration Test (VRPT)Appliance**
Hardware device provisioned and shipped from a Trustwave office	Software device can be downloaded or shipped to Client
1U server form factor, hardened Linux-based appliance	Runs in most recent versions of recent versions of VMware Workstation, VMware Fusion, VMware Server, VMware ESX or even VMware Player
Standard power requirements	Minimum of 512MB of virtual memory, 1 virtual processor and 8 GB of disk space

Trustwave will not utilize a VPN connection to City and County of Denver's internal network. With a VPN approach, much of the actual attack surface of the network cannot be seen by the consultant, resulting in overlooked severe and high-risk security issues.

The RPT or VRPT makes a secured, encrypted outbound connection from City and County of Denver's network to a physically secured and hardened control station located at a Trustwave data center. The Trustwave consultant will be able to access the appliance to conduct testing.

After testing is completed, Trustwave will perform offsite data analysis, facilitate Q&A sessions with City and County of Denver staff regarding internal assessment findings, and provide a final report. Clients shall return the hardware appliance within ten days following the expiration of the term of this Agreement. The consultant will securely destroy any of your data on the appliance at City and County of Denver's request.

About the Remote Penetration Test Appliance

The RPT appliance is an appliance-based server meant to facilitate the type of remote access required to perform a proper internal penetration test. The VRPT appliance provides the same functionality, although this is in the form of a virtual machine (VM) that will run in almost any version of VMware.

Formatted: Font: 9 pt

Formatted: Left

The RPT hardware appliance however is a secured, hardened, appliance platform that will be shipped to City and County of Denver fully configured by the penetration test consultant. The appliance form factor is that of a 1U server with multiple network interfaces. This server should fit in a 1U space on a server rack or desktop.

About the Virtual Remote Penetration Test Appliance

The software-based VRPT appliance is a VM that will be installed on City and County of Denver's own hardware. It requires a minimum of 512MB of virtual memory, 1 virtual processor and 8 GB of disk space. The VRPT can run on most recent versions of VMware Workstation, VMware Fusion, VMware Server, VMware ESX or even VMware Player.

Trustwave will perform Internal Penetration testing at the following City and County of Denver locations:

Number of corporate offices or data centers	3
Are all sites within 50 miles of each other?	Yes

If the RPT remote testing option is chosen City and County of Denver must return the appliance within ten business days after the expiration of the term of this Agreement. If the appliance is not returned within such time, City and County of Denver will incur a charge of $5,000.00 for the appliance.

Phase IV: Onsite Validation Service

As required by the PCI DSS, Trustwave will assign an experienced consultant to validate City and County of Denver's compliance with the data security requirements. The consultant will conduct interviews with key business and operations personnel, and perform required tests as outlined in the PCI DSS version 1.2. Interview questions will be provided prior to Trustwave's arrival. It is anticipated that these meetings will take place over a maximum of two (2) business days during a single onsite visit.

Documentation of Results

At the conclusion of the assessment, a PCI DSS Report on Compliance (ROC) will be created detailing the findings of the assessment and any areas of non-compliance. Specifically, the ROC will include the compliance status with respect to each PCI DSS requirement and recommendations for addressing areas of non-compliance.

Formatted: Font: 9 pt

Formatted: Left

Phase V: Application Penetration Test Service

The PCI DSS requirement 6.6 states that an organization's web-based applications must undergo an application code review each year. The PCI Security Standards Council (SSC) has ruled that an acceptable alternative to an application code review is a manual web application penetration assessment. Trustwave offers this through the Application Penetration Test service. This test determines whether an application is sufficiently secure from an application-layer perspective. The objective of an application penetration test is to determine if the application is vulnerable to an actionable application-level attack from an external attacker. This level of testing validates corporate security policy and development standards by attempting to identify how resilient the web application is to determined attackers. The product of an application penetration test is a report that documents the web application's existing security posture, identifies specific weaknesses and vulnerabilities, and provides purpose built exploit code examples that tell a compelling story of risk from any given vulnerability, and makes recommendations for their remediation.

Benefits of an application penetration test include:

- Identification of the web application's exposure to security risks.
- Identification of specific vulnerabilities affecting the web application.

  Validation and verification of existing security controls, policies and procedures by impartial, third-party experts.

The following illustrates some of the different vulnerability classes Trustwave covers during an application penetration test. This list is not intended to be exhaustive and the actual testing performed depends on the specifics of the application being assessed.

Formatted: Font: 9 pt

Formatted: Left

Authentication and Authorization	➢ Unlimited Login Attempts ➢ Insufficient Authentication ➢ Insufficient Authorization
Session Management	➢ Session Prediction ➢ Session Hijacking ➢ Session Replay ➢ Insufficient Session Expiration
Injection	➢ OS Command Injection ➢ SQL Injection ➢ Cross-site Scripting ➢ LDAP Injection ➢ HTML Injection
Cryptography	➢ Algorithm ➢ Key Management
Logical Attacks	➢ Abuse of Functionality
Data Protection	➢ Transport ➢ Storage
Information Disclosure	➢ Directory Indexing ➢ Path Traversal ➢ Verbose Error Messages ➢ HTML Comments
Bounds Checking	➢ Stack-based ➢ Heap-based ➢ Format String ➢ Integer Overflow/Underflow

Trustwave will utilize varying combinations of application testing approaches. Those approaches are:

Review of the Application Utilizing Trustwave Testing Suite

Using Trustwave's application testing suite, the Trustwave Application Security Team will review the entire web-based application for security related flaws. The Trustwave tools will pinpoint common web application vulnerabilities within the application. Depending upon application design and source code availability, this review will either occur via an offline review of the application source code or a network-based probe of the application.

Vulnerability Scan of the Infrastructure

Using Trustwave's infrastructure testing suite, the Trustwave Application Security Team will review the server infrastructure for common security vulnerabilities. The Trustwave tools will pinpoint infrastructure issues that may undermine the security posture of the application.

Targeted Manual Application Testing

Using Trustwave's targeted manual testing methodology, the Trustwave Application Security Team will manually probe and test targeted aspects of the web-based application. This testing is designed to pinpoint flaws that are as of yet unknown. Traditionally, automated testing fails to uncover these

Formatted: Font: 9 pt

Formatted: Left

types of flaws due to their unique attack logic. Using expert, manual analysis of the application, Trustwave is able to target high-risk areas of the application for manual review.

Full Manual Application Testing

Using Trustwave's full manual testing methodology, the Trustwave Application Security Team will manually probe and test all aspects of a credentialed or non-credentialed application. This type of testing may be performed on any type of application (including web-based and non-web based applications). Using manual analysis of the application, Trustwave is able to provide a higher level of assurance for an application. In the event that the application supports user roles, individual roles will be tested to ensure that logical role isolation exists.

CLIENT may choose from basic to advanced application penetration testing services. The following chart describes the three tier levels of services offered:

Application Tier	Review of Application Utilizing Trustwave Testing Suite	Vulnerability Scan of Infrastructure	Full Manual Testing (including Un-credentialed, and user- and role-based Credentialed Testing)
Tier 4	YES	YES	YES

Phase VI: On-Demand Security Awareness Education (SAE) Portal

Trustwave's on-demand SAE Portal allows organizations to deliver web-based security awareness training to employees and provides tracking of trainee progress. The portal will provide CLIENT with the ability to:

- Track course progress and completion for each course participant.
- Generate reports on trainee progress on a module by module basis as well as quiz results.
- Assign staff managers and administrators roles to help monitor and manage the security awareness program.

TARGET AUDIENCE(S) AND COURSE(S)

Client has identified the following Security Awareness Education target audiences and courses:

- **Security Awareness for Retail Associates**
- **Security Awareness for Agency Owners and Managers**
- **Security Awareness for Technology Services Employees**

Formatted: Font: 9 pt

Formatted: Left

PROJECT PHASES

Trustwave recommends the following development phases for this project:

Audience Analysis	This phase of the project includes both formal and informal audience analysis with the development of a document that clearly outlines the learning objectives of every module of the training guide and describes the learning activities proposed. Account provisioning only begins after Client stakeholder approval of the Instructional Design Document.
Account Setup & System Configuration	Trustwave's provisioning staff will create all administrative accounts and perform a bulk load of all trainee accounts.
Testing	Client performs basic acceptance testing of accounts, content and reports.
Final Hand-off & Administrator Training	Final Client hand-off and training for administrative staff responsible for trainee support, administration and reporting.

Trustwave Compliance Management Portal (CVS Manager)

Trustwave CVS Manager provides a compliance regulation and security controls knowledge base, coupled with robust workflow and reporting capabilities. CVS Manager enables an efficient assessment process relative to PCI compliance, and automated management of remediation actions and controls testing. The parties agree that Trustwave will use the CVS Manager reporting portal to provide project status, report on compliance remediation management status, and to collect and document results throughout the onsite visit if applicable.

Compliance Management

CVS Manager enables an efficient and effective compliance assessment process. Control measurement and reporting capabilities help to understand how compliance impacts business functions. Key compliance management functionality includes:

- Compliance determination for PCI testing procedures required for compliance
- Centralized management of evidence

Formatted: Font: 9 pt

Formatted: Left

- Comprehensive remediation management workflow, including prioritization, remediation planning and review of implementation evidence supporting closure of non-compliant findings
- Integrated dash-boarding, showing compliance validation impact from multiple compliance activities, including required vulnerability scans and annual penetration testing

Powerful Workflow Automation

CVS Manager eliminates inefficient manual processes by automating risk and controls assessment, remediation and control-testing functions:

- Consistent Web-based interface for assessment activities
- Automatically tracks deficiencies and remediation actions, and issues reminders and escalations
- Assessment activities include built-in validity checks and forced collection of evidence where appropriate

CVS Manager portal features include:

- Program management
- Workflow
- Survey management
- Document management
- Remediation management
- Test plan management for verification and audit
- Web-based user interface
- Pre-built reporting for current assessment status, and the final Report on Compliance

Trusted Commerce℠ Security Seal

With the Compliance Validation Service, City and County of Denver receives the Trusted Commerce seal. Displaying the Trusted Commerce seal on the City and County of Denver website will raise recognition of City and County of Denver'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 City and County of Denver'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 City and County of Denver has completed the required actions for validation of PCI DSS compliance. The seal informs customers that, as a QSA, Trustwave examined City and County of Denver's policies, procedures and technical systems and scanned City and County of Denver payment card environment for vulnerabilities. This statement reassures customers that City and County of Denver protects its payment card information as required by the PCI DSS, as well as reinforces customer trust.

Formatted: Font: 9 pt

Formatted: Left

PRICING

Detailed Pricing Schedule

Trustwave Service	1-Year Term
Compliance Validation Services	$36,506.25/yr.
Penetration Testing Services • **Annual testing on up to 3 applications** ○ **$21,333.33 per application**	$64,000/yr.
Security Awareness Education Services • **500 annual Seat Licenses**	$7,500/yr.

1. **All services selected must be for the identical term.**
2. If the total cost hereunder is less than $15,000.00 per year, Client shall pay the fees upfront prior to the rendition of services. If the total cost hereunder is more than $15,000.00 per year, Trustwave will invoice Client, and Client shall pay $9000.52 per month for 12 months.
3. 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.
4. 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.
5. Proposals are valid for up to sixty days from the date on the cover page.
6. Client shall pay all insurance, shipping, and handling charges, including without limitation, custom charges, taxes, VAT.

Formatted: Font: 9 pt

Formatted: Left

Project Deliverables

Deliverable	Description
Vulnerability Scan Report	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.
Compliance Certificate from TrustKeeper	Upon achieving PCI Compliance, City and County of Denver will be provided with an automatically-generated Compliance Certificate from TrustKeeper.
Trusted Commerce Seal	Upon achieving PCI Compliance, the seal can be downloaded to allow customers to see that City and County of Denver has completed the required actions for validating compliance.
PCI DSS Report on Compliance	At the conclusion of the assessment, a PCI DSS Report on Compliance (ROC) will be created detailing the findings of the assessment and any areas of non-compliance. Specifically, the ROC will include the compliance status with respect to each PCI requirement and recommendations for addressing areas of non-compliance.
Statement of Compliance	Upon achieving PCI Compliance, City and County of Denver will be provided with a Statement of Compliance letter.
External Penetration Test Report	Detailing the findings of the manual verification and analysis of discovered vulnerabilities. Findings will be delivered via PenTest Manager, including results and recommendations of tactical and strategic nature.
Internal Penetration Test Report	Detailing the findings of the manual verification and analysis of discovered vulnerabilities. Findings will be delivered via PenTest Manager, including results and recommendations of tactical and strategic nature.
Application Penetration Test Report	After the conclusion of the application testing, findings will be delivered via PenTest Manager, including results and recommendations of tactical and strategic nature.

Formatted: Font: 9 pt

Formatted: Left

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	CLIENT
Name:	Alyssa White
Title:	Cash Management Analyst
Phone/Fax:	720-913-9346
E-mail Address:	Alyssa.white@denvergov.org
Billing Address:	201 W Colfax Ave Denver Co 80202

Formatted: Font: 9 pt

Formatted: Left

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. The parties agree to delete clause 42(a) of the Agreement dated October 23, 2007 and replace it with the following:

   42.a. CONSULTANT SHALL NOT BE LIABLE TO THE CITY FOR (1) ANY ACTS OR OMISSIONS WHICH ARE NOT THE RESULT OF CONSULTANT'S NEGLIGENCE, RECKLESSNESS OR WILLFUL MISCONDUCT, (2) ANY AMOUNTS IN EXCESS OF ONE AND HALF TIMES THE FEES PAID TO CONSULTANT BY THE CITY HEREUNDER, (3) ANY OUTAGES OR SLOW DOWNS OF THE CITY'S COMPUTER SYSTEMS RESULTING FROM THE PERFORMANCE OF ANY SERVICES, UNLESS SUCH OUTAGES OR SLOW DOWNS ARE THE RESULT OF CONSULTANT'S NEGLIGENCE, RECKLESSNESS OR WILLFUL MISCONDUCT, OR (4) ANY LOSSES, COSTS, DAMAGES OR EXPENSES INCURRED BY THE CITY RESULTING FROM THE PERFORMANCE OF ANY TEST, UNLESS SUCH ARE THE RESULT OF CONSULTANT'S NEGLIGENCE OR WILLFUL MISCONDUCT. Section 42(a)(2) shall not limit Consultant's liability for its indemnification obligation to the City (i) for Consultant's breach of its confidentiality obligation to the City and (ii) for Consultant's infringement of a third party's intellectual property rights. Consultant's indemnification obligations hereunder, other than those listed in the preceding sentence, shall be limited to one million dollars ($1,000,000).

~~5.~~6. All other terms and conditions shall remain in full force and effect.

{SIGNATURE PAGE FOLLOWS}

Formatted: Indent: Left: 1", No bullets or numbering

Formatted: Font: 9 pt

Formatted: Left

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 Addition for the designated services and term as accepted by Client:

Signature: _____

Print Name: _____

Title: _____

Effective Date: _____

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

Tick requested services and desired term:

Requested Service	1 Year Term
Compliance Validation Services	
Penetration Testing Services • **Annual testing on up to 3 applications** ○ **$21,333.33 per application**	
Security Awareness Education Services • **500 annual Seat Licenses**	

Signature: _____

Print Name: _____

Title: _____

Date: _____

Formatted: Font: 9 pt

Formatted: Left

Contract Control Number:

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at Denver, Colorado as of

SEAL

CITY AND COUNTY OF DENVER

ATTEST:

By_____

_____

APPROVED AS TO FORM:

REGISTERED AND COUNTERSIGNED:

By_____

By_____

By_____

Contract Control Number: FINAN CE

Contractor Name: TRUSTWAVE HOLDINGS INC

Robert J McCullen

By: _____

AEL by JD

Name: Robert J. McCullen
(please print)

Title: CEO
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)