SIXTH AMENDATORY AGREEMENT

SIXTH 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 75 Remittance Drive, Suite 6000, Chicago, IL 60675-6000 (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, May 25, 2011, April 24, 2012 and on May 3, 2013 (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 extend the agreement and update the scope of work; 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 "…Exhibits A, A-1, A-2 and A-3…" in the existing Agreement shall be amended to read: "…Exhibit A, A-1, A-2, A-3 and A-4 as applicable…". The scope of work marked as Exhibit A-4 is attached and incorporated by reference.

2. 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 July 31, 2015 (the "Term").

3. This Sixth Amendatory Agreement may be executed in counterparts, each of which shall be deemed to be an original, and all of which, taken together, shall constitute one and the same instrument.

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

EXHIBIT LIST:

EXHIBIT A-4 – SCOPE OF WORK

[SIGNATURE PAGES FOLLOW]

EXHIBIT A-4

Addition to the Statement of Work

Presented To: **City and County of Denver**

Presented On: 6/17/2014

Prepared By:

Alexandria Sundahl

ASundahl@trustwave.com

Tel: 312.470.8605

Addition – Exhibit A-4

This is an Addition ("Addendum"), 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.

Addendum Purpose:

The purpose of this Addition is to renew the services listed.

Service Start Date:

The services under this Addendum shall commence as of the date executed below and will expire at the end of the one-year contract Term.

Compliance Validation

Compliance Validation Service (CVS)

Trustwave will provide Client with a Compliance Validation Service designed to help manage the overall compliance process and aid in achieving the business or compliance objectives.

Trustwave QSAs and trained security experts will support Client throughout the CVS process

This team includes:

- **Trustwave Compliance Council** - Trustwave does not allow an individual QSA to determine the compliance status of either a requirement interpretation, or the construction of a compensating control, without first going through a "vetting" process that may involve a team of Senior Consultants, Managing Consultants, an Internal Compliance Council, or all of the above.
- Once documented, a request for interpretation or suitability will be approved by Trustwave, not the individual assessor, thereby maintaining both continuity and consistency throughout the course of the assessment.
- **Onsite Assessor** – Trustwave will assign a Qualified Security Assessor who is the primary resource for the fulfilment of the service. This is the individual who will conduct the onsite validation of compliance for the environment and will be responsible for the following:
- Schedule agreement and conducting the onsite assessment activities
- Compilation of assessment data into the initial report
- Delivery of the any report deliverables, unless otherwise specified

TrustKeeper Support

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 DSS compliance or vulnerability scanning results.

Project Phases and Chronology

Compliance Validation Service consists of Project Initiation and four CVS Phases, and to ensure comprehensive and efficient service, the Client must fulfill their obligations within each phase 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 in this contract. The Compliance Validation Service does not include remediation services. If Client wishes to receive any remediation services, Client must specifically select those services.

Project Initiation: Project Kickoff

- Kickoff meeting between all designated stakeholders
- Discussion and agreement on the Project Definition Plan deliverables and responsibility
- Initial engagement with TW team resources
- Formal scope agreement

CVS Phase I: Scope and Primary Document Collection

- Collect Primary Scoping Documents
- Draft Remediation Tracking Matrix, Report on Compliance (RoC) development
- Online Questionnaire through TrustKeeper©

CVS Phase II: Policy Collection and Mapping (Parallel with Phase I)

- Policy and procedure validation/verification
- External vulnerability scan definition
- Continued draft RoC development

CVS Phase III: Onsite Assessment

- Onsite assessment
- Identification of remediation action items
- Guidance for Client-generated remediation plans (as necessary)
- Scheduling coordination for external penetration testing (if applicable)
- Continued development of the RoC

CVS Phase IV: RoC Finalization and Quality Assurance

- Additional onsite validation (as necessary/if required)
- RoC completion and submission to Trustwave Quality Assurance (QA) team
- RoC review and submission (as required)

External Vulnerability Scanning Service – Up to 260 IP Addresses

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 Approve Scan Vendor (ASV) requirements. You are entitled to receive monthly scans against your PCI environment during the term of the Agreement.

Trusted Commerce Security Seal

With your service, you receive the Trusted Commerce seal. Displaying the Trusted Commerce seal on your Web site confirms your enrollment in Trustwave's program to validate compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Trustwave Compliance Management Portal (Compliance Manager)

Compliance Management

Compliance 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
- 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
- Real-Time Compliance Progress & QA Visibility

Workflow Automation

Compliance Manager automation of a risk and controls assessment, remediation and control-testing functions:

- Web-based interface for assessment activities
- Automatic tracking of deficiencies, remediation actions, and issues reminders and escalations

- Built-in validity checks and forced collection of evidence

Portal Features:

- Web-based user interface
- Program management
- Remediation management
- Document management
- Pre-built reporting for current assessment status, and the final Report on Compliance

Penetration Testing Approach

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 the Client. 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.

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 WebLogic 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 Client's key security contacts on specific system findings and intended target list to be used in the attack phase.

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.

System Vulnerability Exploitation

If the plan of attack devised in the previous step includes any techniques that may impact production systems and infrastructure, Client is first advised of the possible system downtime that may arise. At this point it is up to the Client 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 Client 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 we were able to achieve either of these objectives. If successful exploitation leads SpiderLabs to systems compromise, SpiderLabs consultants will report the breach to Client's key security personnel immediately.

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.

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 Client's key security contacts on the applications identified, and what will be tested. Trustwave will explain the plan of attack for each system and general techniques that will be used. If the system is a production system, Client 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.

Compromise

As systems or applications are compromised, Client's key security contacts will be notified. At that time, the Client contacts will be 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.

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.

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. 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.

External Network Penetration Test Service

PCI DSS requirement 11.3 states that penetration tests must be conducted at least annually or after any significant change to Client's 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(s):

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 will be provided documenting the findings and high-level recommendations to assist 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. Trustwave strongly recommends full-disclosure of the testing to all individuals responsible for the network and related services and devices. Although Trustwave will take precautions to minimize the negative impact on Client systems, there is no 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 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.

Internal Network Penetration Test Service

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. This includes any internal network and system that stores, processes or transmits cardholder data. The objective of an internal network 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 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.

Benefits of an internal penetration test include:

- Identification of the internal network's exposure to security risks
- Identification of specific vulnerabilities affecting the network
- Validation and verification of existing network security controls, policies and procedures by impartial, third-party experts

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

Layer 2 Attacks

- VLAN hopping
- ARP cache poisoning
- Insufficient segmentation and access control
- Exploitation of weaknesses within the switched architecture related to trunking, STP, or failover protocols

Layer 3 Attacks

- IP redirection
- Session hijacking

- ☐ Session replay
- ☐ Password capture

Network / Operating System Layer Attacks

- ☐ Network hash passing
- ☐ Exploitation of DHCP weaknesses
- ☐ Microsoft, Novell, Unix weaknesses

Logical Attacks

- ☐ Abuse of functionality

Cryptography

- ☐ Algorithm
- ☐ Key management

Data Protection

- ☐ Transport
- ☐ Storage

Buffer Overflow

- ☐ Stack-based
- ☐ Heap-based
- ☐ Format string
- ☐ Protocol Fuzzing

Trustwave will perform Internal Penetration Test service at the following Client locations:

Number of Corporate offices, data centers or warehouses	**3**
• **All Sites are within 50 miles of each other**	
If the remote testing option is chosen, the appliance must be returned within five business days of completion of the test. If the appliance is not returned within that time, Client will incur a charge of $5,000.00 for the appliance.	

Remote Testing Option

Client may choose to have the internal penetration testing performed remotely. The consultant will work with Client to ship one of Trustwave's Secure Remote Internal Penetration Testing Appliances to facilitate the remote access needed to conduct the penetration test.

The consultant will first arrange a call to discuss the test parameters and gather all the needed technical information required to configure the appliance. The consultant will then fully configure the appliance and ship it to Client. At this point, Client will simply connect power and the primary interface to the data network. In case of any problems, the appliance has an out-of-band modem connection available that can be connected to a DID phone line to facilitate access for the consultant to troubleshoot and fix the problem.

The appliance makes a secured, encrypted outbound connection from Client's network to a physically secured and hardened control station located at the Trustwave Security Operations Center (SOC). The Trustwave consultant will be able to access the appliance and conduct testing.

After testing is completed, there may be offsite data analysis, Q&A sessions with Client staff regarding findings. The final report will then be presented to for Client's review. The consultant will also securely destroy any data on the appliance and ask that Client ship it back to Trustwave within five (5) business days. Within five (5) 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, the appliance to TRUSTWAVE. Client shall retain the risk of loss until such appliance is delivered to TRUSTWAVE's premises. Client shall be solely responsible for, and shall reimburse TRUSTWAVE for, any damage caused to the appliance while at Client's facilities, except to the extent such damage is caused by TRUSTWAVE personnel. If the appliance is not returned within five (5) days or is 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 appliance. Client shall pay all insurance, shipping, and handling charges, including without limitation, custom charges, taxes, and VAT.

About the Internal Penetration Test Appliance

The Internal Penetration Test Appliance is a secure appliance-based server meant to facilitate the type of remote access required to perform a proper internal penetration test.

Functionally, the appliance is significantly better than a VPN connection to Client's internal network as with a VPN much of the actual attack surface of the network cannot be seen by the consultant. In this way, very severe, very high-risk issues can be missed. Because of these shortcomings with VPN access, Trustwave cannot perform an internal penetration test remotely over a VPN.

The appliance however is a secured, hardened, appliance platform that will be shipped to Client fully configured by the penetration test consultant. Once the appliance is connected the Client network, it will initiate a secure encrypted outbound connection to Trustwave's control server granting remote access to the penetration test consultant.

Most sites that allow basic outbound services such as HTTP/HTTPS will not require any sort of firewall or infrastructure changes to accommodate the appliance.

Additionally, the appliance has a secondary out-of-band modem-based connection available in case of unforeseen problems with outbound access in the environment or environments that do not support any Internet connectivity.

Trustwave Application Penetration Testing

Service Description

The Trustwave SpiderLabs Application Penetration Test service results in an in-depth test of the entire target application and provides a detailed deliverable with both tactical and strategic recommendations to improve the security posture of the target environment. These recommendations are both actionable and advisory in nature and are presented to the customer.

The process involves methodical and expert driven testing of the target application to determine if the application is vulnerable to application layer security risks.

This level of testing helps validate the application layer security controls; the security effectiveness of software development and deployment standards by determining how resilient the application is to determined attackers.

The product of an Application Penetration Test is a report that documents the application's existing security posture, identifies specific weaknesses and vulnerabilities, and provides purpose-built exploit code examples. The detailed report tells a compelling story of risk associated with each vulnerability and makes specific recommendations for their remediation.

Benefits of an Application Penetration Test include:

- Identification of the application's exposure to security risks
- Identification of specific vulnerabilities affecting the application
- Validation and verification of existing security controls, policies, and procedures by impartial third-party experts

The following table lists a number of the different vulnerability classes Trustwave SpiderLabs 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.

Authentication and Authorization	• Unlimited Login Attempts • Authentication Bypass • Authorization Bypass • Default / Weak Passwords

Session Management	• Session Identifier Prediction • Session Hijacking • Session Replay • Session Fixation • Insufficient Session Expiration
Injection	• SQL Injection • Cross-Site Scripting • LDAP Injection • HTML Injection • XML Injection • OS Command Injection
Application Resource Handling	• Path Traversal • Predictable Object Identifiers • XML Entity Expansion • Local & Remote File Inclusion
Cryptography	• Weak Algorithms • Poor Key Management
Logical Attacks	• Abuse of Functionality • Workflow Bypass
Data Protection	• Transport • Storage
Information Disclosure	• Directory Indexing • Verbose Error Messages • HTML Comments • Default Content
Bounds Checking	• Stack-Based • Heap-Based • Format String • Integer Overflow/Underflow

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

Vulnerability Scan of the Application Layer

Using the Trustwave SpiderLabs application testing suite, the entire application will be reviewed for security-related flaws. The tools will identify common application vulnerabilities within the application. Depending upon application design and source code availability, this review will occur either via an offline review of the application source code, or via live interaction with the application.

Vulnerability Scan of the Infrastructure Layer

Using the Trustwave SpiderLabs infrastructure testing suite the application's server infrastructure will be reviewed for common security vulnerabilities. The Trustwave tools will identify common infrastructure issues that may undermine the security posture of the application.

Targeted Manual Application Testing

The Trustwave SpiderLabs targeted manual testing methodology ensures that application is manually probed and penetration tested. This testing is manual and expert driven in nature, specifically designed to identify

vulnerabilities unique to the targeted application. Traditionally, automated testing fails to uncover these, and many other, types of flaws due to the unique attack logic required to identify and/or exploit them. Using this expert, manual analysis of the application, it is possible to target high-risk areas of the application for manual review. In the event that the application supports user roles, individual roles will be tested to ensure that logical role isolation exists. Targeted areas of the application are tested to the extent allowed by testing time constraints and prioritized by criticality of application components, data sensitivity and likelihood of exploitation.

Full Manual Application Testing

Using our full manual testing methodology, Trustwave SpiderLabs will manually probe and test all aspects of the 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, all individual roles will be tested to ensure that logical role isolation exists.

The following chart describes the five tier levels of service that may be selected for each application that requires testing:

Test Tier	Automated Application Review	Vulnerability Scan of Infrastructure	Manual Verification of All Findings	Targeted Manual Application Testing	Full Manual Testing
Tier 0	YES	YES	YES	NO	NO
Tier 1	YES	YES	YES	YES, 6 hours	NO
Tier 2	YES	YES	YES	YES, 16 hours	NO
Tier 3	YES	YES	YES	YES, 40 hours	NO
Tier 4	YES	YES	YES	NO	YES

On-Demand Security Awareness Education (SAE) Portal – 500 seats

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

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.

Pricing

Trustwave Service	1-Year Term
Compliance Validation Service (CVS) including: • TrustKeeper Scanning for up to 260 IP Addresses • 1 Report on Compliance • On-site Validation • Internal and External Network Penetration Test Service • Trusted Commerce Security Seal **1 Tier 2 Application Penetration Test** • Full review of application utilizing Trustwave testing suite • 16 Hours of manual application penetration test	$57,839
Security Awareness Training • 500 Annual Seat Licenses	$7,500
TOTAL:	**$5,444.92/month** **$65,339.00**

1. Trustwave will invoice Client, and Client shall pay $5,444.92 per month for 12 months. All fees quoted and payments shall be in USD and exclusive of taxes.
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 effectively as possible given timing and travel requirements. Valid expenses typically include parking, meals, lodging, photocopying, communication costs, airfare, mileage and 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 USD and exclusive of taxes. 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 other services.
4. Proposals are valid for up to sixty (60) days from the date on the cover page.
5. Annualized services must be used each year during the term and cannot be used and/or credited in subsequent years.
6. Client shall pay all shipping, handling, and related charges, including and without limitation taxes and customs charges.

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 point-of-contact (POC) as identified above, or a 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 or any other applicable requirements. Client is solely responsible for providing access to and coordinating any required interviews or testing with its 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 or any other applicable 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 Trustwave and a mutually acceptable testing schedule shall be agreed upon.
6. 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.
7. Client is responsible to notify Trustwave of any changes or cancellations relevant to an on-site visit, no less than 10 business days in advance. In the event Client cancels an on-site visit less than 48 hours prior to such visit, in addition to reimbursing Trustwave for any travel and expenses actually incurred, Client shall pay Trustwave a cancelled visit fee in the amount of 5% of the fees.

Contact Information

Client's Primary Contact

Name: Alyssa White

Title: Cash Administrator

Phone: 720-913-9346

Email: Alyssa.white@denvergov.org

Address: 201 W Colfax Ave, Denver, CO 80202

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 hereby provide and accept this Agreement.

Signature: _____

Print Name: _____

Title: _____

Effective Date: _____

City and County of Denver: As a duly authorized representative with the authority to enter into agreements and contracts on behalf of Client, I hereby accept this Agreement for the designated services.

Signature: _____

Print Name: _____

Title: _____

Date: _____

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-CE74035-06

Contractor Name: TRUSTWAVE HOLDINGS INC

Signature: Robert J McCullen

Print Name: Robert J McCullen

Title: Chief Executive Officer

Date: August 11, 2014

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)