

AMENDATORY AGREEMENT

THIS AMENDATORY AGREEMENT is made between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (“City”), and **TRUSTWAVE HOLDINGS, INC.**, doing business as **TRUSTWAVE**, a Delaware corporation, doing business at 70 W. Madison Street, Suite 600, Chicago, IL 60602, (the Contractor”) as of the date on the signature page below (the “Effective Date”).

WITNESSETH:

WHEREAS, the Parties entered into an Agreement dated December 3, 2015, for the performance of certain services set forth in the Agreement and Addendum to Agreement, collectively the (“Agreement”); and

WHEREAS, the Parties wish to amend the Agreement to extend the term, increase the funding and add a new pricing menu.

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...” in the Agreement shall be amended to read: “...Exhibit A and A-1...” as applicable. The order form, pricing menu, and scoping document marked as Exhibit A-1 attached to this Amendatory Agreement are hereby incorporated by reference.

2. Article 3 of the Agreement entitled “**TERM**” is amended to read as follows:

“**3. TERM:** The Agreement will commence on October 26, 2015, and will expire on December 31, 2021 (the “Term”). Subject to the Executive Director’s prior written authorization, the Contractor shall complete any work in progress as of the expiration date and the Term of the Agreement will extend until the work is completed or earlier terminated by the Executive Director.

3. Article 4. d. (1) of the Agreement entitled “**COMPENSATION AND PAYMENT**”, “**Maximum Contract Amount**” is amended to read as follows:

“**4. COMPENSATION AND PAYMENT:**

d. Maximum Contract Amount:

(1) Notwithstanding any other provision of the Agreement, the City’s maximum payment obligation will not exceed **SEVEN HUNDRED AND EIGHT THOUSAND DOLLARS (\$708,000.00)** (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 Contractor beyond that

specifically described in Exhibit A and A-1. Any services performed beyond those set forth therein are performed at Contractor's risk and without authorization under the Agreement. The Manager may modify the SOW, with the consent of the Contractor, by written authorization provided the maximum contract amount is not exceeded. Notwithstanding anything else in this Agreement or otherwise, in the event of any changes or updates to applicable laws, regulations, rules, standards, Interpretations or other external guidelines (including without limitation the PCI Data Security Standard or the Payment Application Data Security Standard), Contractor may, upon notice to the City, make appropriate revisions to the scope and pricing for any Services that are affected by such changes or updates. In the event the parties cannot come to an agreement on the new scope and pricing, either party may terminate this Agreement without penalty.”

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

5. This Amendatory Agreement is not effective or binding on the City until it has been fully executed by all required signatories of the City and County of Denver, and if required by Charter, approved by the City Council.

[SIGNATURE PAGES FOLLOW

Contract Control Number: FINAN-201951370-01 [ALFRESCO 201522955-01]
Contractor Name: TRUSTWAVE HOLDINGS INC

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

SEAL **CITY AND COUNTY OF DENVER:**

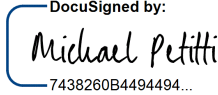
ATTEST: By: _____

APPROVED AS TO FORM: **REGISTERED AND COUNTERSIGNED:**
Attorney for the City and County of Denver
By: _____ By: _____

By: _____

Contract Control Number:
Contractor Name:

FINAN-201951370-01 [ALFRESCO 201522955-01]
TRUSTWAVE HOLDINGS INC

By: _____

Name: Michael Petitti
(please print)

Title: President
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)

**SECURETRUST™ ORDER CONFIRMATION**

Customer	City and County of Denver	Contact Name	Paul Kresser
Proposal/Quote Number	Q-00107591	Phone	7209134876
Order Form Expiration	9/30/2020	Contact Email	paul.kresser@denvergov.org
Sales Representative	Lubna Daimee	Address	Colfax
Payment Terms	Net 30	City	Denver
		State/Province	Colorado
		Country	United States
		Postal Code	80202

COMPLIANCE AND SECURITY SOLUTIONS

Product Name Description	Product Description	Start Date	End Date	Billing Terms	Selling Term
SL-MST-COMPLIANCE	Managed Security Testing Commitment - Total sum of money to be added to client's MST account. - For Compliance Business Unit	10/26/2020	12/31/2021	Monthly	14
GCRS-CVS1 Basic Bundle	PCI DSS Compliance Validation Service - Basic Bundle	10/26/2020	12/31/2021	Monthly	14
GCRS-CVS-PCIRemediation	PCI DSS Remediation Consulting	10/26/2020	12/31/2021	Monthly	14
GCRS-CVS1	PCI DSS Compliance Validation Service	10/26/2020	12/31/2021	Monthly	14
EVS-CVS-SCAN-UNLIMITED	External Vulnerability Scanning- Unlimited Scans	10/26/2020	12/31/2021	Monthly	14

Total Sales Order (USD)

121,951.54

Is a Purchase Order (PO) required for the purchase or payment of the products on this Order Form? (Client to complete)

☐ **NO** I cannot provide a purchase order for the above referenced purchase because my company does not issue purchase orders.

☐ **YES** Please complete below

PO Number	PO Amount

☐ My company is a Tax Exempt Organization EIN: _____

☐ International Tax ID (if applicable) ID: _____

TERMS AND CONDITIONS

The parties acknowledge that they have read and understand this Order Form and agree that it is subject to (1) the terms of the Master Service Agreement (as amended) between the parties listed above ("MSA") or if an MSA has not been executed by Client and Trustwave, this Order Form is subject to the applicable online Master Terms and Conditions ("Online Terms"), (2) the description(s) of the applicable products, services and dependencies ("Descriptions"), (3) the applicable end user license agreements for purchase of software or third party products and/or services ("EULA(s)"), (4) the data protection agreement ("DPA"), and (5) the applicable scoping documents ("Scope") (altogether, the "Agreement"). The terms of the Descriptions, DPA and if applicable, the EULA(s), Scope and/or any Online Terms are incorporated into and made a part of the Agreement by reference. The Online Terms, Descriptions, EULA(s) and DPA are available at <https://www.trustwave.com/en-us/legal-documents/contract-documents/>.

Client agrees to pay Trustwave the fees stated in this Order Form under the terms of the Agreement. Trustwave will invoice Client for these fees upon execution of this Order Form or as otherwise agreed to in this Order Form or the Agreement. Payments will be due and payable within thirty (30) days of the date of receipt of Trustwave's invoice or as otherwise agreed to in this Order Form or the Agreement.

Notwithstanding anything to the contrary in the Agreement, if Client terminates the Agreement or services in this Order Form **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 service charges for the remainder of the term of the Agreement or applicable services.

If this executed Order Form is returned to Trustwave by Client after the Order Start Date above Trustwave may update the Order Start Date to be the date of execution without increasing the Total Fees or the term length. Each party further warrants that it has full corporate power and authority to execute and deliver this Order Form and to perform its obligations hereunder. In Witness whereof, the parties have affixed their signatures and the Order Form is considered effective on the date shown below:

City and County of Denver

Trustwave Holdings, Inc.

Authorized Signature

Authorized Signature

Michael Petitti

Full Name

President, SecureTrust

Title

Full Name

Title

9/2/2020

Effective Date



Exhibit A-1

Scoping Document

PCI DSS Compliance Validation Service –Scope of Work

PCI DSS Compliance Validation Service	
Scope Summary	
Total number of client HQ locations identified in scope	1
Total number of client IT operation locations identified in scope	1
Total number of client data centers identified in scope	2
Total number of client call or care centers identified in scope	1
Total number of client retail facilities identified in scope	113
Total number of POI devices identified in scope	113
Total number of Applications identified in scope	3
Total number of Operating Systems identified in scope	3
Total number of Servers identified in scope	300
Total Number of Work stations identified in scope	551
Total number of Network Devices identified in scope	35
Total number of Databases types identified in scope	1
Total number of People to Interview identified in scope	10
Scope Summary	
Organization Type	Merchant
P2PE Approved Solution?	Yes
Onboard payment application?	Yes
Is the encrypting terminal an approved PIN transaction security (PTS) device?	Yes
Does your organization use more than 1 terminal model?	N/A
If more than 1 terminal model, total number of terminal models	-
If more than 1 terminal model, total number of reports	1

MST PRICING MENU

Below is the full menu of services offered for SpiderLabs MST, each for a 12-month enrollment period and may continue on based on the contract term. While City and County of Denver may only intend to purchase a certain tier of testing, should City and County of Denver elect to purchase another tier of testing, the following pricing in Pricing Tables will apply. Provisioning an MST account requires predefined pricing.

Definitions for the following menus:

- An “application” is defined as a non-web-based or a web-based application.

- 1) A non-web based application is defined as a single piece of software running on a specific piece of hardware. The application may communicate with many infrastructure components (middleware, databases, etc.).
- 2) A web-based application may be distributed across multiple servers; similarly, multiple applications may run on a single website.
- 3) A single web-based application is defined to include only one login page, a unified “look and feel”, a single session tracking mechanism, and a consistent programming language or application framework.

- A “network” is defined as a logical class C network segment of IP addresses accessed from a single point of origination. A “logical class C” is defined as a block of 256 IP addresses. Networks smaller than 256 contiguous IP addresses may be combined to make one logical class C, provided they are accessed from the same point of origination. For example, three network segments of 64 IP addresses each can be combined under one logical class C. Tests are scoped against complete network segments (including routers, network addresses, broadcast addresses, etc.) accessed from a single location (single switch port for internal tests). Potentially unused IP addresses are still considered part of the scope since network penetration testing is performed against at least an entire network segment, and not isolated devices.

Service	Description	Number of Tests	Annual Enrollment
Tier 0 Database Scanning 1 Target One Scan	Cloud-based database scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE One (1) Managed Database Assessment Scan	1300.00 /database
Tier 0 Database Scanning 1 Target Quarterly Scans	Cloud-based database scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE Four (4) Managed Database Assessment Scan	2500.00 /database
Tier 0 Database Scanning 1 Target Monthly Scans	Cloud-based managed database scanning that will perform the minimum required checks to meet compliance requirements. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE Twelve (12) Managed Database Assessment Scan	6500.00 /database
Tier 0 Database Scanning 1 Target Weekly Scans	Cloud-based database scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE Fifty Two (52) Managed Database Assessment Scan	19500.00 /database

NETWORK SCANNING

Service	Description	Number of Tests	Annual Enrollment
Tier 0 Network Scanning 256 IP addresses Target One Scan	Cloud-based network scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE One (1) Managed Network Assessment Scan	1300.00 /network
Tier 0 Network Scanning 256 IP addresses Target Quarterly Scans	Cloud-based network scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE Four (4) Managed Network Assessment Scan	2500.00 /network
Tier 0 Network Scanning 256 IP addresses Target Monthly Scans	Cloud-based network scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE Twelve (12) Managed Network Assessment Scan	6500.00 /network
Tier 0 Network Scanning 256 IP addresses Target Weekly Scans	Cloud-based network scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE Fifty-Two (52) Network Assessment Scan	19500.00 /network

APPLICATION SCANNING

Service	Description	Number of Tests	Annual Enrollment
Tier 0 Application Scanning 1 Target One Scan	Cloud-based application scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE One (1) Managed Application Assessment Scan	1300.00 /application
Tier 0 Application Scanning 1 Target Quarterly Scans	Cloud-based application scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE Four (4) Managed Application Assessment Scans	2500.00 /application
Tier 0 Application Scanning 1 Target Monthly Scans	Cloud-based application scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE Twelve (12) Managed Application Assessment Scan	6500.00 /application
Tier 0 Application Scanning 1 Target Weekly Scans	Cloud-based application scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The	SKU: SL-MST-CYBER Or	19500.00

	client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.	SL-MST-COMPLIANCE Fifty Two (52) Application Assessment Scans	/application
--	--	--	--------------

NETWORK PENETRATION TESTING

Network Service	Description	Number of Tests	Annual Enrollment
Single Network Tier 2 Test	Tier 2 Network Test: Opportunistic Threats —This test will build upon the basic test described above and simulate an opportunistic attack executed by a skilled attacker that does not spend an extensive amount of time executing highly sophisticated attacks. This type of attacker seeks easy targets (“low-hanging fruit”) and will use a mix of automated tools and manual exploitation to penetrate their targets.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE One (1) Network Tier 2 Opportunistic Threat Test	4800.00 /network
Tier 1 Basic Test	Managed Network Best Practices Assessment Scans Tier 1 Network Test: Basic Test —This test will simulate a basic attack executed by an attacker of limited sophistication with minimal skills. This class of attacker (often referred to as “script kiddies”) typically use freely available automated attack tools.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE Four (4) Managed Network Best Practices Assessment Scans One (1) Network Tier 1 Basic Test	7500.00 /network
Tier 2 Opportunistic Threats Test	Managed Network Best Practices Assessment Scans	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE	13,000.00

	Tier 2 Network Test: Opportunistic Threats —This test will build upon the basic test described above and simulate an opportunistic attack executed by a skilled attacker that does not spend an extensive amount of time executing highly sophisticated attacks. This type of attacker seeks easy targets ("low-hanging fruit") and will use a mix of automated tools and manual exploitation to penetrate their targets.	Four (4) Managed Network Best Practices Assessment Scans One (1) Network Tier 2 Opportunistic Threat Test	/network
Tier 3 Targeted Threats Test	Managed Network Best Practices Assessment Scans Tier 3 Network Test: Targeted Threats — This test will simulate a targeted attack executed by a skilled, patient attacker that has targeted a specific organization. This class of attacker will expend significant effort trying to compromise an organization's systems.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE Four (4) Managed Network Best Practices Assessment Scans One (1) Network Tier 3 Targeted Threat Test Includes Uncredentialed Testing	17000.00 /network
Tier 4 Advanced Threats Test	Managed Network Best Practices Assessment Scans Tier 4 Network Test: Advanced Threats — This test will simulate an advanced attack executed by a highly motivated, well-funded and extremely sophisticated attacker who will exhaust all options for compromise before relenting.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE Four (4) Managed Network Best Practices Assessment Scans One (1) Network Tier 4 Advanced Threat Test Includes Uncredentialed Testing	25000.00 /network

APPLICATION PENETRATION TESTING

Application Service	Description	Number of Tests	Annual Enrollment
Single Application Penetration Test-Tier 2	Tier 2 Application Test: Opportunistic Threats —This test will build upon the basic test described above and simulate an opportunistic attack executed by a skilled attacker that does not spend an extensive	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE	4800.00

	amount of time executing highly sophisticated attacks. This type of attacker seeks easy targets ("low-hanging fruit") and will use a mix of automated tools and manual exploitation to penetrate their targets.	One (1) Application Tier 2 Opportunistic Threat Test	/application
Tier 1 Basic Test	<p>Managed Application Best Practices Assessment Scans</p> <p>Tier 1 Application Test: Basic Test—This test will simulate a basic attack executed by an attacker of limited sophistication with minimal skills. This class of attacker (often referred to as "script kiddies") typically use freely available automated attack tools.</p>	<p>SKU: SL-MST-CYBER</p> <p>Or</p> <p>SL-MST-COMPLIANCE</p> <p>Four (4) Managed Application Best Practices Assessment Scans</p> <p>One (1) Application Tier 1 Basic Test</p>	<p>7500.00</p> <p>/application</p>
Tier 2 Opportunistic Threats Test	<p>Managed Application Best Practices Assessment Scans</p> <p>Tier 2 Application Test: Opportunistic Threats—This test will build upon the basic test described above and simulate an opportunistic attack executed by a skilled attacker that does not spend an extensive amount of time executing highly sophisticated attacks. This type of attacker seeks easy targets ("low-hanging fruit") and will use a mix of automated tools and manual exploitation to penetrate their targets.</p>	<p>SKU: SL-MST-CYBER</p> <p>Or</p> <p>SL-MST-COMPLIANCE</p> <p>Four (4) Managed Application Best Practices Assessment Scans. One (1) Application Tier 2 Opportunistic Threat Test</p>	<p>13000.00</p> <p>/application</p>
Tier 3 Targeted Threats Test	<p>Managed Application Best Practices Assessment Scans</p> <p>Tier 3 Application Test: Targeted Threats—This test will simulate a targeted attack executed by a skilled, patient attacker that has targeted a specific organization. This class of attacker will expend significant effort trying to compromise an organization's systems.</p>	<p>SKU: SL-MST-CYBER</p> <p>Or</p> <p>SL-MST-COMPLIANCE</p> <p>Four (4) Managed Application Best Practices Assessment Scans</p>	<p>17000.00</p> <p>/application</p>

		One (1) Application Tier 3 Targeted Threat Test Includes Uncredentialed Testing	
Tier 4 Advanced Threats Test	Managed Application Best Practices Assessment Scans Tier 4 Application Test: Advanced Threats —This test will simulate an advanced attack executed by a highly motivated, well-funded and extremely sophisticated attacker who will exhaust all options for compromise before relenting.	SKU: SL-MST-CYBER Or SL-MST-COMPLIANCE Four (4) Managed Application Best Practices Assessment Scans One (1) Application Tier 4 Advanced Threat Test Includes Uncredentialed Testing	25000.00 /application

ADDITIONAL IPs

For network MST testing, Client may add additional IP addresses in excess of 256 subject to payment of the following additional fees:

Hosts to Add to Enrollment	Price per Host
32, 64	0.4% of enrollment fee
96, 128	0.35% of enrollment fee
160, 224	0.3% of enrollment fee
256, 288...480	0.25% of enrollment fee
512...992	0.2% of enrollment fee
1024...2496	0.15% of enrollment fee
2528...4096	0.1% of enrollment fee
4128...9984	0.08% of enrollment fee

THE FOLLOWING TERMS SHALL APPLY TO MST SERVICES ONLY:

- The term of the MST services under this Agreement (the "MST Services") shall be 1 year from the effective date of this Agreement (the "Subscription Period").
- Client hereby agrees to pay Trustwave **\$36,308.00 USD** (the "Fees") for the right to subscribe for MST Services during the Subscription Period up to the amount of the Fees. During the Subscription Period, Client will be given an account to Trustwave's Managed Security Testing Portal where in Client will have the ability to enroll an application or network segment in the MST Services.
- The Fees will be invoiced monthly during the Subscription Period.
- If the Subscription Period is longer than one year, then at the end of each year during the Subscription Period Trustwave shall invoice and Client shall pay for all MST Services for which Client has subscribed in the MST Portal but remain unpaid for that year.
- In the event Client wishes to purchase additional MST Services in excess of the Fees listed herein during the Subscription Period, Client may issue a purchase order to Trustwave that references this Agreement with the applicable additional Fees stated therein. Any such additional Fees will be invoiced up front and will not be billed subscription. The parties may renew or extend the Subscription Period by entering into an addendum to this Agreement that is signed by both parties.
- Any MST Services ordered in the final year of the Subscription Period for which delivery has begun will continue to be performed after the expiration of the Subscription Period, and this Agreement shall remain in effect until all such MST Services have been completed. If Client does not utilize the enrolled MST Services (or any portion thereof) during the applicable 12-month enrollment period for such MST Services, such unused MST Services cannot be used and/or credited in subsequent years. Any remaining unused MST Services at the end of the Subscription Period cannot be used and/or credited in subsequent years.

Scoping

1 Internal Network Penetration Testing Tier 2 overage of 608 IPs = \$28,808.00
1 External Network Penetration Testing Tier 1 standard = \$7,500.00
TOTAL MST FUNDS \$36,308.00 USD

Client's Initial MST Account Administrator

This individual will be the initial account holder in Trustwave's Managed Security Testing Portal and will be able to (i) enroll targets in the MST program (i.e., deplete the MST account balance) and (ii) create other accounts in the Portal with varying levels of authority (which can include enrolling targets and depleting the MST account balance). This role may be transferred at any time.

Name: _____

Title: _____

Phone: _____

Fax: _____

Email: _____