Administered by
UNIVERSITY OF MAINE SYSTEM
Office of Strategic Procurement

REQUEST FOR PROPOSALS (RFP)

ON-CALL IDENTITY PROTECTION SERVICES
University of Maine System

RFP # 20-13

ISSUE DATE:
April 4, 2013

PROPOSALS MUST BE RECEIVED BY:
May 7, 2013

DELIVER PROPOSALS TO:

University of Maine System
Office of Strategic Procurement
Attn: Hal Wells
16 Central Street
Bangor, ME 04401

SECTION ONE

1.0 GENERAL INFORMATION:

1.1 Purpose: The University of Maine System is seeking proposals for the provision of on-call identity protection services.

This Request for Proposals (RFP) states the instructions for submitting proposals, the procedure and criteria by which a vendor may be selected and the contractual terms by which the University intends to govern the relationship between it and the selected vendor.

1.2 Definition of Parties: The University of Maine System will hereinafter be referred to as the "University." Respondents to the RFP shall be referred to as "Bidder(s)" or "bidder(s)". The Bidder to whom the Contract is awarded shall be referred to as the "Contractor."

1.3 Scope: In the event of a security breach or unauthorized disclosure the University may require identity protection services. It is the University's intent to establish open contracts with bidders who, in the sole discretion of the University, have the experience, qualifications, staff and training to respond to a breach or unauthorized disclosure. Award is not a guarantee of work. Contracts shall cover the actual needs of the University as determined by The Office of Information Security.

1.4 Evaluation Criteria: Proposals will be evaluated on many criteria deemed to be in the University's best interests, including, but not limited to:

1.4.1 Demonstrated ability (experience, qualifications, staff and training) to provide identity protection services as described in this RFP.

1.4.2 Cost of service for each quantity tier (e.g. between 1 – 500 persons would be x dollars, etc.).

1.4.3 Ability to meet specifications.

1.4.4 References.

1.5 Communication with the University: It is the responsibility of the bidder to inquire about any requirement of this RFP that is not understood. Responses to inquiries, if they change or clarify the RFP in a substantial manner, will be forwarded by addenda to all parties that have received a copy of the RFP. Addenda will also be posted on our web site, www.maine.edu/strategic/upcoming_bids.php. It is the responsibility of all bidders to check the web site before submitting a response to ensure that they have all pertinent documents. The University will not be bound by oral responses to inquiries or written responses other than addenda.

Inquiries must be made to: Hal Wells
Office of Strategic Procurement
University of Maine System
16 Central Street
Bangor, Maine 04401
(207) 973-3302
hcwells@maine.edu

The deadline for inquires is April 24, 2013.

The University will respond to written inquiries not later than close of business, April 30, 2013.

1.6 Award of Proposal: Presentations may be requested of two or more bidders deemed by the University to be the best suited among those submitting proposals on the basis of the selection criteria. After presentations have been conducted, the University may select the bidder(s) which, in its opinion, has made the proposal that is the most responsive and most responsible and may award the Contract to that/those bidders. The University reserves the right to waive minor irregularities. Scholarships, donations, or gifts to the University, will not be considered in the evaluation of proposals. The University reserves the right to reject any or all proposals, in whole or in part, and is not necessarily bound to accept the lowest cost proposal if that proposal is contrary to the best interests of the University. The University may cancel this Request for Proposals or reject any or all proposals in whole or in part. Should the University determine in its sole discretion that only one bidder is fully qualified, or that one bidder is clearly more qualified than any other under consideration, a contract may be awarded to that bidder without further action.

1.7 Award Protest: Bidders may appeal the award decision by submitting a written protest to the University of Maine System's Director of Strategic Procurement within five (5) business days of the date of the award notice, with a copy of the protest to the successful bidder. The protest must contain a statement of the basis for the challenge.

1.8 Confidentiality: The information contained in proposals submitted for the University's consideration will be held in confidence until all evaluations are concluded and an award has been made. At that time, the winning proposal will be available for public inspection. Pricing and other information that is an integral part of the offer cannot be considered confidential after an award has been made. The University will honor requests for confidentiality for information of a proprietary nature to the extent allowed by law. Clearly mark any information considered confidential.

The University must adhere to the provisions of the Maine Freedom of Access Act (FOAA), 1 MRSA §401 et seq. As a condition of accepting a contract under this section, a contractor must accept that, to the extent required by the Maine FOAA, responses to this solicitation, and any ensuing contractual documents, are considered public records and therefore are subject to freedom of access requests.

1.9 Costs of Preparation: Bidder assumes all costs of preparation of the proposal and any presentations necessary to the proposal process.

1.10 Debarment: Submission of a signed proposal in response to this solicitation is certification that your firm (or any subcontractor) is not currently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from participation in this transaction by any State or Federal department or agency. Submission is also agreement that the University will be notified of any change in this status.

1.11 Proposal Understanding: By submitting a proposal, the bidder agrees and assures that the specifications are adequate, and the bidder accepts the terms and conditions herein. Any exceptions should be noted in your response.

1.12 Proposal Validity: Unless specified otherwise, all proposals shall be valid for ninety (90) days from the due date of the proposal.

1.13 Non-Responsive Proposals: The University will not consider non-responsive proposals, i.e., those with material deficiencies, omissions, errors or inconsistencies.

1.14 Specification Protest Process and Remedies: If a bidder feels that the specifications are written in a way that limits competition, a specification protest may be sent to the Office of Strategic Procurement. Specification Protests will be responded to within five (5) business days of receipt. Determination of protest validity is at the sole discretion of the University. The due date of the proposal may be changed if necessary to allow consideration of the protest and issuance of any necessary addenda. Specification protests shall be presented to the University in writing as soon as identified, but no less than five (5) business days prior to the bid opening date and time. No protest against the award due to the specifications shall be considered after this deadline. Protests shall include the reason for the protest and any proposed changes to the specifications. Protests should be delivered to the Office of Strategic Procurement in sealed envelopes, clearly marked as follows:

SPECIFICATION PROTEST, RFP #20-13

1.15 Proposal Submission: A **SIGNED** original and three (3) copies (FOUR TOTAL) **PLUS ONE VIRUS FREE ELECTRONIC COPY** of the proposal must be submitted to the Office of Strategic Procurement, University of Maine System, 16 Central Street, Bangor, Maine 04401, in a sealed envelope by **Tuesday, May 7, 2013**, to be date stamped by the Office of Strategic Procurement in order to be considered. Normal business hours are 8:00 a.m. to 5:00 p.m., Monday through Friday. **The ELECTRONIC COPY of the proposal must be provided on CD or flash drive with the complete narrative and attachments in Adobe Acrobat or MS Word.** Bidders may wish to check http://www.maine.edu/alerts/ to determine if University operations have been suspended. Proposals received after the due date will be returned unopened. There will be no public opening of proposals (see Confidentiality clause). In the event of suspended University operations, proposals will be due the next business day. Vendors are strongly encouraged to submit proposals in advance of the due date to avoid the possibility of missing the due date because of unforeseen circumstances. Vendors assume the risk of the methods of dispatch chosen. The University assumes no responsibility for delays caused by any package or mail delivery service. Postmarking by the due date WILL NOT substitute for receipt of proposal. Additional time will not be granted to any single vendor, however additional time may be granted to all vendors when the University determines that circumstances require it. **FAXED OR E-MAIL PROPOSALS WILL NOT BE ACCEPTED**. The envelope must be **clearly** identified on the outside as follows:

Name of Bidder
Address of Bidder
Due Date
RFP #20-13

1.16 Authorization: Any contract or agreement for services that will, or may, result in the expenditure by the University of $50,000 or more must be approved in writing by the Director of Strategic Procurement and it is not approved, valid or effective until such written approval is granted.

SECTION TWO

2.0 GENERAL TERMS AND CONDITIONS:

2.1 Contract Administration: The Office of Information Security or its designee shall be the University's authorized representative in all matters pertaining to the administration of this Contract.

2.2 Contract Documents: If a separate contract is not written, the Contract entered into by the parties shall consist of the RFP, the signed proposal submitted by the Contractor, the specifications including all modifications thereof, and a purchase order or letter of agreement requiring signatures of the University and the Contractor, all of which shall be referred to collectively as the Contract Documents.

2.3 Contract Modification and Amendment: The parties may adjust the specific terms of this Contract (except for pricing) where circumstances beyond the control of either party require modification or amendment. Any modification or amendment proposed by the Contractor must be in writing to the Contract Administrator. Any agreed upon modification or amendment must be in writing and signed by both parties.

2.4 Contract Term: The initial term shall be for a period of two (2) years commencing upon the issuance of written letters of notification. With mutual written agreement of the parties this Contract may be extended for three (3) additional one-year periods.

Quoted pricing shall be firm for the initial term.

2.5 Contract Data: The Contractor is required to provide the University with detailed data concerning the Contract at the completion of each contract year or at the request of the University at other times.

2.6 Contract Validity: In the event one or more clauses of the Contract are declared invalid, void, unenforceable or illegal, that shall not affect the validity of the remaining portions of the Contract.

2.7 Non-Waiver of Defaults: Any failure of the University to enforce or require the strict keeping and performance of any of the terms and conditions of this Contract shall not constitute a waiver of such terms, conditions, or rights.

2.8 Cancellation/Termination: If the Contractor defaults in its agreement to provide personnel or equipment to the University's satisfaction, or in any other way fails to provide service in accordance with the contract terms, the University shall promptly notify the Contractor of such default and if adequate correction is not made within twenty-four hours the University may take whatever action it deems necessary to provide alternate services and may, at its option, immediately cancel this Contract with written notice. Cancellation does not release the Contractor from its obligation to provide goods or services per the terms of the Contract during the notification period.

2.9 Employees: The Contractor shall employ only competent and satisfactory personnel and shall provide a sufficient number of employees to perform the required services efficiently and in a manner satisfactory to the University. If the Contract Administrator or designee, notifies the Contractor in writing that any person employed on this Contract is incompetent, disorderly, or otherwise unsatisfactory, such person shall not again be employed in the execution of this Contract without the prior written consent of the Contract Administrator.

2.10 Clarification of Responsibilities: If the Contractor needs clarification of or deviation from the terms of the Contract, it is the Contractor's responsibility to obtain written clarification or approval from the Contract Administrator.

2.11 Litigation: This Contract and the rights and obligations of the parties hereunder shall be governed by and construed in accordance with the laws of the State of Maine without reference to its conflicts of laws principles. The Contractor agrees that any litigation, action or proceeding arising out of this Contract, shall be instituted in a state court located in the State of Maine.

2.12 Assignment: Neither party of the Contract shall assign the Contract without the prior written consent of the other, nor shall the Contractor assign any money due or to become due without the prior written consent of the University.

2.13 Equal Opportunity: In the execution of the Contract, the Contractor and all subcontractors agree, consistent with University policy, not to discriminate on the grounds of race, color, religion, sex, sexual orientation, including transgender status or gender expression, national origin or citizenship status, age, disability, genetic information, or veteran's status and to provide reasonable accommodations to qualified individuals with disabilities upon request. The University encourages the employment of individuals with disabilities.

2.14 Independent Contractor: Whether the Contractor is a corporation, partnership, other legal entity, or an individual, the Contractor is an independent contractor. If the Contractor is an individual, the Contractor's duties will be performed with the understanding that the Contractor is a self-employed person, has special expertise as to the services which the Contractor is to perform and is customarily engaged in the independent performance of the same or similar services for others. The manner in which the services are performed shall be controlled by the Contractor; however, the nature of the services and the results to be achieved shall be specified by the University. The Contractor is not to be deemed an employee or agent of the University and has no authority to make any binding commitments or obligations on behalf of the University except as expressly provided herein. The University has prepared specific guidelines to be used for contractual agreements with individuals (not corporations or partnerships) who are not considered employees of the University.

2.15 Sexual Harassment: The University is committed to providing a positive environment for all students and staff. Sexual harassment, whether intentional or not, undermines the quality of this educational and working climate. The University thus has a legal and ethical responsibility to ensure that all students and employees can learn and work in an environment free of sexual harassment. Consistent with the state and federal law, this right to freedom from sexual harassment was defined as University policy by the Board of Trustees. Failure to comply with this policy could result in termination of this Contract without advanced notice. Further information regarding this policy is available from the Director of Equity and Diversity, (207) 973-3372.

2.16 Indemnification: The Contractor agrees to be responsible for, and to protect, save harmless, and indemnify the University and its employees from and against all loss, damage, cost and expense (including attorney's fees) suffered or sustained by the University or for which the University may be held or become liable by reason of injury (including death) to persons or property or other causes whatsoever, in connection with the operations of the Contractor or any subcontractor under this agreement.

2.17 Contractor's Liability Insurance: During the term of this agreement, the Contractor shall maintain the following insurance:

Insurance Type	Coverage Limit
1. Commercial General Liability (Written on an Occurrence-based form)	$1,000,000 per occurrence or more (Bodily Injury and Property Damage)
2. Vehicle Liability (Including Hired & Non-Owned)	$1,000,000 per occurrence or more (Bodily Injury and Property Damage)
3. Workers Compensation (In Compliance with Applicable State Law)	Required for all personnel

The University of Maine System shall be named as Additional Insured on the Commercial General Liability insurance.

Certificates of Insurance for all of the above insurance shall be filed with:

Office of Strategic Procurement
University of Maine System
16 Central Street
Bangor, Maine 04401

Certificates shall be filed prior to the date of performance under this Agreement. Said certificates, in addition to proof of coverage, shall contain the standard statement pertaining to written notification in the event of cancellation, with a thirty (30) day notification period.

As additional insured and certificate holder, the University should be included as follows:

University of Maine System
16 Central Street
Bangor, Maine 04401

2.18 Smoking Policy: The University must comply with the "Workplace Smoking Act of 1985" and M.R.S.A. title 22, § 1541 et seq "Smoking Prohibited in Public Places." In compliance with this law, the University has prohibited smoking in all University System buildings except in designated smoking areas. This rule must also apply to all contractors and workers in existing University System buildings. The Contractor shall be responsible for the implementation and enforcement of this requirement within existing buildings.

2.19 Gramm Leach Bliley (GLB) Act (Confidentiality of Information): The Contractor shall comply with all aspects of the GLB Act regarding safeguarding confidential information.

2.20 Payments: Payment will be upon submittal of an invoice to the address shown on the Purchase Order by the Contractor on a Net 30 basis unless discount terms are offered. Invoices must include a purchase order number. The University is using several, preferred methods of payment: Bank of America's ePayables and PayMode electronic payment systems. Please indicate your ability to accept payment via any or all of these methods.

SECTION THREE

3.0 SPECIFICATIONS: The University requires identity protection services in the event of a security breach or unauthorized disclosure. The University reserves the right to determine what level of service will be used and whether or not any services will be used on an incident-by-incident basis. The baseline will likely be comprised of identity protection services.

3.1 Identity Protection: The minimum requirements for identity protection services are:

3.1.1 Tiered pricing: Vendors will provide pricing per individual (as described in 4.2.1 below) using the University's tiered pricing scheme (e.g., between 1 – 500 persons would be X amount of dollars, etc…). Pricing shall remain firm for the initial term.

3.1.2 Ability to provide identity protection to include:

- Credit Report monitoring – daily monitoring from 1, 2, or 3 major credit bureaus.
- Identity monitoring (e.g., web crawling that searches the web underground to detect illegal selling of personal information - SSN, Credit and Debit Card number, phone number, email address).
- Identity theft insurance.
- Live phone support for customers.
- Identity repair / recovery assistance.

3.1.3 Ability to provide "one-offs" where protection services can be provided in the event that a security incident affects one individual.

3.1.4 Ability to provide mailing notification services.

3.1.5 Ability to provide address lookup services.

3.1.6 Ability to provide one or more of the multiple ways for the end user to enroll (e.g., phone, web, mail).

3.1.7 Ability to respond 24/7, 365 days/year

SECTION FOUR

4.0 PROPOSAL CONTENT:

Bidders shall ensure that all information required herein is submitted with the proposal. All information provided should be verifiable by documentation requested by the University. Failure to provide all information, inaccuracy or misstatement may be sufficient cause for rejection of the proposal or rescission of an award. Bidders are encouraged to provide any additional information describing operational abilities. Responses to each requirement below should be in order and clearly marked with the section number to which they respond.

4.1 Business Profile:

4.1.1 **No financial statements are required to be submitted with your proposals,** however, prior to an award the University may request financial statements from your company, credit reports and letters from your bank and suppliers.

4.1.2 **Please submit with your proposal** a detailed history and description of your company and any published reports about your company.

4.2 Pricing:

4.2.1 The University would prefer vendor responses that respond using the University's table, below. However if your pricing scheme cannot conform to the University's tiered pricing, please feel free to provide your firm's pricing scheme.

Provide base enrollment costs per subscriber for a one year enrollment using the University's tiered scheme, below.

Number of Subscribers	Base Price per Subscription
1 – 100	
101 – 500	
501 – 1,000	
1,001 – 2,500	
2,501 – 10,000	
10,001 – 25,000	
25,001 +	

Describe how you charge per subscription.

4.2.2 Provide the additional cost per person for each additional service offered (customer address lookup, customer mailing, color printing, enrollment method, length of protection coverage, etc.) if applicable.

4.2.3 Provide the cost/savings of providing **credit report monitoring** from 1, 2, or 3 of the major credit bureaus; as well as having this completed on a daily or monthly basis, if applicable.

4.2.4 Provide the cost/savings of providing **credit history reports** to the customer via email, mail, or online; if they want the report from 1, 2, or 3 of the major credit bureaus; and if they want it on a monthly or annual basis.

4.2.5 Provide the costs of obtaining live vendor help/support beyond typical business hours (e.g., 24 hour support), if applicable.

4.2.6 Pricing shall be firm for the initial (two year) term of the contract.

4.3 Functionality:

4.3.1 Describe what is provided to the customer in terms of identity protection and the length (term) of each form of protection.

4.3.2 Describe which pieces of information are protected (e.g., social security number, driver's license number, bank account information, etc.).

4.3.3 Describe how you provide credit history reports. Does the customer receive a copy of their credit report via email, mail, or online? Do they receive it from one, two, or three reporting agencies? Can the customer get that on a monthly or annual basis?

4.3.4 Describe credit report monitoring: specifically, whether the use of one or three bureaus is utilized and if monitoring is done on a daily or monthly basis.

4.3.5 Describe how you assist in identity repair / recovery assistance. Do you only provide the resources or do you complete necessary paperwork and make the phone calls?

4.3.6 Describe how you provide mailing notification services. How you deal with returned mail and if you provide the option for the University to determine who returned mail goes to.

4.3.7 Describe the process you use for address lookup services to include the criteria you use for lookup (e.g., first/last name, SSN, birth date) and what service you subscribe to. If a third party service is utilized describe the methods of protecting data transferred between you and the third party.

4.3.8 Describe the ways in which a customer can enroll in identity protection.

4.3.9 Describe the enrollment duration (window of time) the University can offer a customer to enroll in identity protection services once notified.

4.3.10 Describe method(s) of how customer's personally identifiable information is safely transferred from the University to you. Describe the protections you use to safeguard the data. As part of the agreement, Standards for Safeguarding Information (Attachment A) are included. Describe how you comply with its requirements.

4.3.11 Describe your customer phone help/support. Is live support provided during regular business hours? If yes, then define what these hours would be. Or is live support provided 24 hours a day?

4.3.12 Describe how you will work with the University in the event of a breach. What is the process and turn-around time from first contact from the University until the affected person's notification via mail?

4.4 Payment Method: Indicate your ability to accept electronic payments. (Section 2.20)

4.5 References: Provide three references. These references should be agencies your firm has done business with in the past year **on projects with a similar scope to this one**. Provide company names with contact person, telephone number and email address.

SIGNATURE PAGE

COMPANY NAME: _____

By: _____
(Signature)

_____
(Print Name)

_____
(Title)

_____
(Phone)

_____
(Cell Phone)

_____
(E-mail Address)

_____
(Date)

ATTACHMENT A

UNIVERSITY OF MAINE SYSTEM
STANDARDS FOR SAFEGUARDING INFORMATION

This Attachment addresses the Contractor's responsibility for safeguarding Compliant Data and Business Sensitive Information consistent with the University of Maine System's Information Security Policy and Standards. (infosecurity.maine.edu)

Compliant Data is defined as data that the University needs to protect in accordance with statute, contract, law or agreement. Examples include Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Biley Act (GLBA), Maine Notice of Risk to Personal Data Act, and the Payment Card Industry Data Security Standards (PCI-DSS).

Business Sensitive Information is defined as data which is not subject to statutory or contractual obligations but where the compromise or exposure of the information could result in damage or loss to the University.

1. Standards for Safeguarding Information: The Contractor agrees to implement reasonable and appropriate security measures to protect all systems that transmit, store or process Compliant Data and Business Sensitive Information or personally identifiable information from Compliant Data and Business Sensitive Information furnished by the University, or collected by the Contractor on behalf of the University, against loss of data, unauthorized use or disclosure, and take measures to adequately protect against unauthorized access and malware in the course of this engagement.

   A. Compliant Data and Business Sensitive Information may include, but is not limited to names, addresses, phone numbers, financial information, bank account and credit card numbers, other employee and student personal information (including their academic record, etc.), Drivers License and Social Security numbers, in both paper and electronic format.

   B. If information pertaining to student educational records is accessed, transferred, stored or processed by Contractor; Contractor shall protect such data in accordance with FERPA.

   C. If information pertaining to protected health information is accessed, used, collected, transferred, stored or processed by Contractor; Contractor shall protect such data in

accordance with HIPAA and Contractor shall sign and adhere to a Business Associate Agreement.

D. If Contractor engages in electronic commerce on behalf of the University or cardholder data relating to University activities is accessed, transferred, stored or processed by Contractor; Contractor shall protect such data in accordance with current PCI-DSS guidelines.

E. If information pertaining to protected "Customer Financial Information" is accessed, transferred, stored or processed by Contractor; Contractor shall protect such data in accordance with GLBA.

2. Prohibition of Unauthorized Use or Disclosure of Information: Contractor agrees to hold all information in strict confidence. Contractor shall not use or disclose information received from, or created or received by, Contractor on behalf of the University except as permitted or required by this Agreement, as required by law, or as otherwise authorized in writing by the University.

3. Return or Destruction of Compliant or Business Sensitive Information:

A. Except as provided in Section 3(B), upon termination, cancellation, or expiration of the Agreement, for any reason, Contractor shall cease and desist all uses and disclosures of Compliant Data or Business Sensitive Information and shall immediately return or destroy (if the University gives written permission to destroy) in a reasonable manner all such information received from the University, or created or received by Contractor on behalf of the University, provided, however, that Contractor shall reasonably cooperate with the University to ensure that no original information records are destroyed. This provision shall apply to information that is in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of University information, including any compilations derived from and allowing identification of any individual's confidential information. Except as provided in Section 3(B), Contractor shall return (or destroy) information within 30 days after termination, cancellation, or expiration of this Agreement.

B. In the event that Contractor determines that returning or destroying any such information is infeasible, Contractor shall provide to University notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of such information is infeasible, Contractor shall extend the protections of this Agreement to such information and limit further uses and disclosures of such information to those

purposes that make the return or destruction infeasible, for so long as Contractor maintains such information.

C. Contractor shall wipe or securely delete Compliant Data or Business Sensitive Information and personally identifiable information furnished by the University from storage media when no longer needed. Measures taken shall be commensurate with the standard for "clearing" as specified in the National Institute of Standards and Technology (NIST) Special Publication SP800-88: Guidelines for Media Sanitization, prior to disposal or reuse.

4. Term and Termination:

A. This Attachment shall take effect upon execution and shall be in effect commensurate with the term of the Agreement

5. Subcontractors and Agents: If Contractor provides any Compliant Data or Business Sensitive Information received from the University, or created or received by Contractor on behalf of the University, to a subcontractor or agent, the Contractor shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Contractor by this Agreement.

6. Contractor shall control access to University data: All Contractor employees shall be adequately screened, commensurate with the sensitivity of their jobs. Contractor agrees to limit employee access to data on a need-to-know basis. Contractor shall impose a disciplinary process for employees not following privacy procedures. Contractor shall have a process to remove access to University data immediately upon termination or re-assignment of an employee by the Contractor.

7. Unless otherwise stated in the agreement, all Compliant Data or Business Sensitive Information is the property of the University and shall be turned over to the University upon request.

8. Contractor shall not amend or replace hardware, software or data without prior authorization of the University.

9. If mobile devices are used in the performance of this Agreement to access University Compliant Data or Business Sensitive Information, Contractor shall install and activate authentication and encryption capabilities on each mobile device in use.

10. Reporting of Unauthorized Disclosures or Misuse of Information: Contractor shall report to the University any use or disclosure of Compliant Data or Business Sensitive Information not authorized by this Agreement or in writing by

the University. Contractor shall make the report to the University not more than one (1) business day after Contractor learns of such use or disclosure. Contractor's report shall identify; (i) the nature of the unauthorized use or disclosure, (ii) the information used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Contractor has done or shall do to mitigate the effects of the unauthorized use or disclosure, and (v) what corrective action Contractor has taken or shall take to prevent future similar unauthorized use or disclosure. Contractor shall provide such other information, including a written report, as reasonably requested by the University. Contractor shall keep University informed on the progress of each step of the incident response. Contractor shall indemnify and hold University harmless from all liabilities, costs and damages arising out of or in any manner connected with the security breach or unauthorized use or disclosure by Contractor of any University Compliant Data or Business Sensitive Information. Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a security breach or use or disclosure of Compliant Data or Business Sensitive Information by Contractor in violation of the requirements of this Agreement. In addition to the rights of the Parties established by this Agreement, if the University reasonably determines in good faith that Contractor has materially breached any of its obligations, the University, in its sole discretion, shall have the right to:

- Inspect the data that has not been safeguarded and thus has resulted in the material breach, and/or
- Require Contractor to submit a plan of monitoring and reporting, as the University may determine necessary to maintain compliance with this Agreement;
- and/or Terminate the Agreement immediately.

11. Survival: The respective rights and obligations of Contractor under Section 12 of the Agreement or Section 3 of this Attachment shall survive the termination of this Agreement.

12. Contractor Hosted Data: If Contractor hosts University Compliant Data or Business Sensitive Information in or on Contractor facilities, the following additional clauses should be used.

A. Contactor computers that host University Compliant Data or Business Sensitive Information shall be housed in secure areas that have adequate walls and entry control such as a card controlled entry or staffed reception desk. Only

authorized personnel shall be allowed to enter and visitor entry will be strictly controlled.

B. Contractor shall design and apply physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters. Contractor shall protect hosted systems with Uninterruptible Power Supply (UPS) devices sufficient to meet business continuity requirements.

C. Contractor shall backup systems or media stored at a separate location with incremental back-ups at least daily and full back-ups at least weekly. Incremental and full back-ups shall be retained for 15 days and 45 days respectively. Contractor shall test restore procedures not less than once per year.

D. Contractor shall provide for reasonable and adequate protection on its network and system to include firewall and intrusion detection/prevention.

E. Contractor shall use strong encryption and certificate-based authentication on any server hosting on-line and e-commerce transactions with the University to ensure the confidentiality and non-repudiation of the transaction while crossing networks.

F. The installation or modification of software on systems containing University Compliant Data or Business Sensitive Information shall be subject to formal change management procedures and segregation of duties requirements.

G. Contractor who hosts University Compliant Data or Business Sensitive Information shall engage an independent third-party auditor to evaluate the information security controls not less than every two (2) years. Such evaluations shall be made available to the University upon request.

13. <u>If Contractor employees work under University Management direction</u>, Contractor employees will receive security awareness training and be subject to the same information security standards as University employees. If the Contractor accesses University systems, Contractor shall agree to the University's Acceptable Use Policy.

14. <u>If the Contractor provides system development,</u> Compliant Data or Business Sensitive Information shall not be used in the development or test environments. Records that contain these types of data elements may be used if that data is first de-identified, masked or altered so that the original value is not recoverable. For programs that process University data, initial implementation as well as applied updates and modifications must be produced from specifically authorized and trusted program source libraries and personnel.

Contractor shall provide documentation of a risk assessment of new system development or changes to a system.

UNIVERSITY

By: _____ _____

Signature Date

_____

Printed

_____ _____

Title Address

CONTRACTOR

By: _____ _____

Signature Date

_____

Printed

_____ _____

Title Address