ATTACHMENT G

PRIVACY AND DATA PROTECTION

During the course of providing Products and Services, Supplier may be provided access to or otherwise obtain or handle Waste Management Data (as defined below). Supplier agrees to protect all Waste Management Data as detailed herein. In the event of any conflict or other inconsistency between this Attachment and any provision contained within the body of the Agreement, this Attachment shall take precedence and control.

1. Definitions. For purposes herein, the following definitions shall apply:

(a) "Cardholder Data" means: (i) with respect to a payment card, the account holder's name, account number, service code, card validation code/value, PIN or PIN block, valid to and from dates and magnetic stripe data; and (ii) information relating to a payment card transaction that is identifiable with a specific account.

(b) "Data Protection Requirements" means, collectively, all national, state and local laws or regulations relating to the protection of Personally Identifiable Information in the jurisdictions in which Waste Management Entities do business and that apply with respect to Supplier's handling of Waste Management Data (including, without limitation, in the United States, the Gramm-Leach-Bliley Act and in Canada, the Personal Information Protection and Electronic Documents Act).

(c) "Internal Data" means any information regarding the business or business activities of Waste Management or Waste Management Entities (as defined below) that is not available to the general public, but which does not qualify as Personally Identifiable Data. For the avoidance of doubt, unless such information otherwise meets the definition of Cardholder Data, Personally Identifiable Data, or Special Personally Identifiable Data, Internal Data includes, without limitation, all information the Waste Management Entities may possess that is subject to an obligation to maintain the confidentiality of same. Supplier's treatment of Internal Data may be subject to a separate agreement.

(d) "PCI Standards" means the security standards for the protection of payment card data with which the payment card companies require merchants to comply, including, but not limited to, the Payment Card Industry Data Security Standards currently in effect and as may be updated from time to time.

(e) "Personally Identifiable Data" means any information that identifies or can be used to identify an individual or can be used to authenticate an individual. Personally Identifiable Data includes, without limitation, names, signatures, addresses, telephone numbers, fax numbers, e-mail addresses, place of birth, driver's license number, images of driver's licenses, Internet Protocol ("IP") address, passport number, credit card information, membership reward program information and affiliations with companies or associations and information about transactions with Waste Management Entities, including, without limitation, Special Personally Identifiable Data.

(f) "Special Personally Identifiable Data" means: (i) Social Security number, Taxpayer Identification Number, passport number, driver's license number or other government-issued identification number; or (ii) financial account number, credit card number, debit card number credit report information, with or without any code or password that would permit access to the account; or (iii) an individual's race, religion, ethnicity, medical or health information, biometric data (e.g. fingerprints, retina scans, etc.), digital signature files (i.e. digital identification key not a scanned image of a person's signature on paper), background check information or sexual orientation; and/or (iv) Cardholder Data.

(g) "Waste Management Data" means any Personally Identifiable Data, Special Personally Identifiable Data, and/or Internal Data. For the avoidance of doubt, to the extent the designation of any data or information as Personally Identifiable Data, Special Personally Identifiable Data, and/or Internal Data in this Attachment conflicts with any definition of confidential information within the body of the Agreement, to the fullest extent possible, such conflict shall be interpreted as this Attachment imposing additional or supplemental responsibilities and obligations in connection with such information and not as creating a conflict therewith. To the extent any such conflict cannot be resolved in accordance with the preceding sentence, this Attachment shall take precedence and control over any conflict.

(h) "Waste Management Entities" means, collectively, Waste Management, Inc. and all companies in which Waste Management, Inc. directly or indirectly owns a majority interest, commonly called "subsidiaries" of Waste Management, Inc.

2. All references herein to Waste Management Data, Personally Identifiable Data, Special Personally Identifiable Data, Cardholder Data and Internal Data are to data that is provided to, or obtained, used, accessed, maintained or otherwise handled by Supplier in connection with providing Products and Services to Waste Management.

3. Supplier will at all times comply with and treat Waste Management Data in accordance with the requirements of this Attachment and the Data Protection Requirements. Supplier hereby represents and warrants that it will inform itself regarding, and comply with, all applicable Data Protection Requirements. Supplier will notify Waste Management in the event that Supplier believes that Waste Management's instructions concerning Waste Management Data, including, without limitation, the requirements of this Attachment, would cause Supplier to violate any Data Protection Requirement.

4. At no time shall Supplier acquire any ownership, license, rights, title or other interest in or to Waste Management Data, all of which shall, as between Waste Management and Supplier, be and remain the proprietary and confidential information of Waste Management. Supplier shall not be entitled to use Waste Management Data for its own purposes or for the purpose of any third party. In no event may Supplier: (a) use Waste Management Data to market its services or those of a third party; or (b) sell or rent Waste Management Data to third parties.

5. Supplier will hold Waste Management Data in strict confidence and will not, except as may be permitted pursuant to this Section, disclose Waste Management Data to any third party, firm or enterprise (including, without limitation, Supplier's affiliates) or use (directly or indirectly) any Waste Management Data for any purpose other than as specifically directed by Waste Management in writing and in accordance with the Data Protection Requirements. In addition, Supplier may not physically transfer Waste Management Data to, or allow access to Personally Identifiable Data by, its employees or personnel, including, without limitation, any third party, firm or enterprise (including, without limitation, Supplier's affiliates) in any location outside the United States without first receiving Waste Management's prior written consent.

6. Before providing Waste Management Data to any third party, including, without limitation, Supplier's affiliates or a potential subcontractor or service provider, Supplier must obtain written approval for such disclosure from an officer of Waste Management. If Supplier is permitted to disclose Waste Management Data to such third party, such disclosure must be limited to the minimum Waste Management Data necessary for the third party to fulfill its obligations to Supplier. Supplier agrees that if Waste Management consents to Supplier's disclosure of Waste Management Data to such third party, prior to making such disclosure, Supplier will enter into a written agreement with the third party that includes obligations that are at least as broad in scope and restrictive as those under this Attachment. Nonetheless, Supplier shall remain at all times accountable and responsible for all actions by such third parties with respect to the disclosed Waste Management Data as if such third parties were a Party to this Agreement.

7. Supplier shall:

(a) develop, implement, maintain, monitor and comply with a comprehensive, written information security program that contains administrative, technical and physical safeguards to protect against anticipated threats or hazards to the security, confidentiality or integrity of, the unauthorized or accidental destruction, loss, alteration or use of, and the unauthorized access to or acquisition of Waste Management Data and provide Waste Management with documentation of such safeguards, upon the reasonable request of Waste Management at any time;

(b) conduct a risk assessment to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of electronic, paper and other records containing Waste Management Data and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks; and

(c) ensure that its information security program is consistent with: (i) Waste Management's information security practices and requirements as may be issued to Supplier by Waste Management from time to time, including, without limitation, enhanced security provisions governing the use of Special Personally Identifiable Data in order to comply with applicable laws; (ii) the Data Protection Requirements; (iii) the PCI Standards, if Supplier has access to or otherwise handles Cardholder Data; and (iv) prevailing industry practices.

8. Supplier shall review and, as appropriate, revise its information security program: (a) at least annually or whenever there is a material change in Supplier's business practices that may reasonably affect the security or integrity of Waste Management Data; (b) in accordance with prevailing industry practices; and (c) as reasonably requested by Waste Management. If Supplier modifies its information security program following such a review, Supplier shall promptly notify Waste Management of the modifications and shall provide the modifications to Waste Management in writing upon Waste Management's request. Supplier may not alter or modify its information security program in such a way that will weaken or compromise the confidentiality and security of Waste Management Data.

9. Supplier agrees that: (a) it will establish, maintain and comply with appropriate access controls consistent with then-current industry best practices, which as of the inception of the Agreement, includes, but is not limited to, limiting access to Waste Management Data to the minimum number of Supplier employees and personnel who require such access in order to provide Products and Services to Waste Management; (b) its employees and personnel who will be provided access to, or otherwise come into contact with, Waste Management Data will be required (including during the term of their employment or retention and thereafter) to protect such Waste Management Data in accordance with the requirements of this Attachment; (c) its employees and personnel who will be provided access to, or otherwise come into contact with, Waste Management Data will have the appropriate qualifications and references (which include, without limitation, a requirement that Supplier conduct drug and background checks of such employees and personnel prior to such employees or personnel accessing any Waste Management Data in accordance with Supplier's Safety and Health Declaration) to handle and to protect such Waste Management Data in accordance with the requirements of this Attachment; and (d) Supplier will provide such employees and personnel with appropriate training regarding information security and the protection of personally identifiable data.

10. Supplier shall maintain and enforce its information security program at each location from which Supplier provides Products and Services. In addition, Supplier shall ensure that its information security program covers all networks, systems, servers, computers, notebooks, laptops, PDAs, mobile phones, and other devices and media that process or handle Waste Management Data or that provide access to Waste Management Data, or the networks, systems or information of the Waste Management Entities. Moreover, Supplier shall ensure that its information security program includes, without limitation, industry standard password protections, firewalls and anti-virus and malware protections to protect Waste Management Data stored on computer systems. Supplier shall regularly test and monitor Supplier security procedures and systems and shall conduct periodic reviews to ensure compliance with the requirements set forth herein. Supplier shall make the results of such reviews available to Waste Management at Waste Management' request. In addition, Supplier shall annually, at no additional cost or expense to Waste Management: (a) provide Waste Management with a copy of their SSAE16 or equivalent external assessment report, which shall include an assessment report(s) for any third party supporting the Products and Services, (b) complete Waste Management's standard information security questionnaire (at Waste Management's request), which shall include responses to any questions regarding Supplier's controls for any part of the Products and Services performed by a third party by or on behalf of Supplier, and (c) make available an appropriately senior representative of Supplier's information security team to meet with Waste Management's information security team to discuss any questions or concerns Waste Management may have regarding Supplier's information security program.

11. Supplier shall encrypt, using industry standard encryption tools, all records and files containing Waste Management Data that Supplier: (a) transmits or sends wirelessly or across public networks; (b) stores on laptops or storage media; (c) where technically feasible, stores on portable devices; and (d) stores on any device that is transported outside of the physical or logical controls of Supplier. Supplier shall safeguard the security and confidentiality of all encryption keys associated with encrypted Waste Management Data.

12. If Supplier disposes of any paper, electronic or other record containing Waste Management Data, Supplier shall do so by taking all reasonable steps (based on the sensitivity of the Waste Management Data) to destroy the Waste Management Data by: (a) shredding; (b) permanently erasing and deleting; (c) degaussing; or (d) otherwise modifying Waste Management Data in such records to make it unreadable, unreconstructable and indecipherable. All Special Personally Identifiable Data must be disposed of in a manner described in (a) through (c).

13. If Supplier connects to the computing systems or networks of any Waste Management Entities, Supplier agrees that: (a) Supplier will not access, and will not permit any other person or entity to access, the computing systems or networks of the Waste Management Entities without Waste Management's prior written authorization and any such actual or attempted access shall be consistent with any such authorization; (b) all Supplier connectivity to the computing systems and networks of Waste Management Entities and all attempts at same shall be only through Waste Management's security gateways/firewalls; and (c) Supplier will use latest available, most comprehensive virus and malware detection/scanning program prior to any attempt to access any of the computing systems or networks of any Waste Management Entities. Supplier shall inform Waste Management in writing of the identity of any Supplier employees and personnel who have access to the systems or networks of Waste Management Entities. Supplier may change the Supplier employees and personnel who have access to the systems or networks of Waste Management Entities, provided Supplier gives prior written notice to Waste Management and receives Waste Management' written approval for any such change.

14. If Supplier has access to Cardholder Data, Supplier shall: (a) ensure that its information security program addresses the requirements of the PCI Standards; (b) maintain a complete audit trail of all transactions and activities associated with Cardholder Data; and (c) not store card validation codes/values, complete magnetic stripe data or PINs and PIN blocks. Supplier represents and warrants that it shall maintain certification of its compliance with the PCI Standards and that it shall undergo independent, third-party quarterly system vulnerability scans. Supplier shall promptly provide, at the request of Waste Management, current certification of compliance with the PCI Standards, by an authority recognized by the payment card industry for that purpose. If during the Term of the Agreement, Supplier undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PCI Standards and/or other material payment card industry standards, it will promptly notify Waste Management of such circumstances. Supplier further represents and warrants that it shall not take any actions that will compromise Waste Management's ability to comply with the PCI Standards.

15. Waste Management may perform periodic security assessments of the computing systems and networks of Waste Management or Waste Management Entities, which may include, without limitation, assessment of certain portions of the computing systems and networks of Supplier. Supplier agrees that should any such assessment reveal inadequate security by Supplier, Waste Management, in addition to other remedies it may have, may suspend Supplier's access to the computing systems and networks of Waste Management Entities until such inadequate security has been appropriately addressed. Such suspension will not be considered Waste Management's breach of the Agreement.

16. If Supplier is requested or required (by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands or other similar processes) to disclose any Waste Management Data to a third party, Supplier shall immediately notify Waste Management of any such anticipated disclosure (except to the extent otherwise required by applicable law) and shall not disclose Waste Management Data to the third party without providing Waste Management notice at least forty-eight (48) hours following such request or demand, so that Waste Management may, at its own expense, exercise such rights as it may have under law to prevent or limit such disclosure. Notwithstanding the foregoing, Supplier shall exercise commercially reasonable efforts to prevent and limit any such disclosure to only such Waste Management Data as Supplier's legal counsel has determined is required to be produced and to otherwise preserve the confidentiality of Waste Management Data, including, without limitation, by cooperating with Waste Management to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to Waste Management Data.

17. Supplier shall establish and maintain complete and accurate books, notices, and accounting and administrative records necessary to document the proper handling of Waste Management Data under this Agreement, including, without limitation, accounts of all transactions involving Waste Management Data, and shall retain such records pursuant to applicable law. Upon reasonable notice to Supplier, Supplier shall permit Waste Management, its auditors, designated audit representatives, and regulators, including, without limitation, data protection regulators, to audit and inspect, at Waste Management's sole expense (except as provided herein), and no more often than once per year (unless otherwise required by Waste Management's regulators): (a) the facilities of Supplier and any third-party service providers of Supplier previously approved by Waste Management where Waste Management Data is stored or maintained by, or on behalf of, Supplier; (b) any computerized or paper systems used to share, disseminate or otherwise handle Waste Management Data; (c) Supplier's security practices and procedures, facilities, resources, plans and procedures; and (d) all books, notices, and accounting and administrative records required to be retained by Supplier hereunder. Such audit and inspection rights shall be, at a minimum, for the purpose of verifying Supplier's compliance with this Attachment, all applicable Data Protection Requirements and the PCI Standards. If any audit or inspection conducted pursuant to this Agreement reveals a material technical issue, security problem, or other non-compliance with this Attachment, any applicable Data Protection Requirements and/or the PCI Standards, Supplier will pay Waste Management' costs for conducting such audit and/or inspection and will propose an appropriate written response, including, without limitation, a plan for the remediation of the problem, within the time reasonably requested by Waste Management. Upon Waste Management' approval of such plan, Supplier will remedy the problem according to the plan. Waste Management will not be responsible for any additional costs or fees related to such remedy.

18. Supplier shall notify Waste Management promptly in writing (and in any event within five (5) days of receipt) of any communication received from an individual relating to his or her request to access, modify or correct Personally Identifiable Data relating to the individual, and Supplier shall comply with all reasonable instructions of Waste Management before responding to such communications.

19. Upon notice to Supplier, Supplier shall promptly assist and support Waste Management in the event of an investigation by any regulator, including, without limitation, a data protection regulator or similar authority, if and to the extent that such investigation relates to Waste Management Data handled by Supplier. Such assistance and support shall be at Waste Management's sole expense, except where such investigation was required due to Supplier's acts or omissions, in which case, such assistance and support shall be at Supplier's sole expense.

20. Supplier is responsible for any and all information security incidents involving Waste Management Data that is handled by, or on behalf of, Supplier. Supplier shall notify Waste Management in writing immediately (and in any event within twenty-four (24) hours) whenever Supplier reasonably believes that there has been an unauthorized acquisition, destruction, modification, use, or disclosure of, or access to, Waste Management Data ("Breach"). After providing such notice, Supplier will investigate the Breach, take all necessary steps to eliminate or contain the exposures that led to such Breach, document all information collected as part of its investigation of the Breach, and keep Waste Management advised of the status of such Breach and all matters related thereto. Supplier further agrees to provide, at Supplier's sole cost, reasonable assistance and cooperation requested by Waste Management and/or Waste Management's designated representatives, in the furtherance of any correction, remediation, or investigation of any such Breach and/or the mitigation of any damage, including, without limitation, any notification that Waste Management may determine appropriate to send to individuals impacted or potentially impacted by the Breach, and/or the provision of any credit reporting service that Waste Management deems appropriate to provide to such individuals. Unless required by law, Supplier shall not notify any individual or any third party other than law enforcement of any potential Breach involving Waste Management Data without first consulting with, and obtaining the permission of, Waste Management. In addition, within thirty (30) days of identifying or being informed of a Breach, Supplier shall develop and execute a plan, subject to Waste Management's approval, that reduces the likelihood of a recurrence of such Breach. Supplier agrees that Waste Management may at its discretion immediately terminate the Agreement without penalty if a Breach occurs. Supplier agrees that, due to the unique nature of Waste Management Data, the unauthorized disclosure or use of Waste Management Data may cause irreparable harm to Waste Management, the extent of which will be difficult to ascertain and for which there will be no adequate remedy at law. Accordingly, Supplier agrees that Waste Management, in addition to any other available remedies, shall have the right to seek an immediate injunction and other equitable relief enjoining any breach or threatened breach of the provisions of this Attachment without the necessity of posting any bond or other security.

21. At the request of Waste Management, Supplier and any of the Supplier Parties will enter into a data processing agreement that incorporates the European Commission Standard Contractual Clauses between Controllers and Processors, or any similar agreement relating to other countries, with one or more of the Waste Management Entities in order to allow Personally Identifiable Data to be transferred to Supplier and any affiliate or subcontractor of Supplier by Waste Management Entities operating outside the United States.

22. The Parties agree that, to the extent such entity is not a party to the Agreement, each of the Waste Management Entities are intended third party beneficiaries of the privacy and data security provisions of this Agreement and such provisions are intended to inure to the benefit of the Waste Management Entities. Without limiting the foregoing, the Waste Management Entities will be entitled to enforce all privacy and data security provisions of this Agreement as if each was a signatory to this Agreement.

23. Supplier shall, as appropriate, regularly dispose of Waste Management Data that is maintained by Supplier, but that is no longer necessary to provide the Products and Services as set forth in Section 12 above. Notwithstanding the foregoing, Supplier shall comply with Waste Management's written instructions to preserve Waste Management Data in connection with any investigations, lawsuits or other disputes in which any Waste Management Entities may be involved. Except to perform Termination Support as outlined in Section 24 below, upon termination or expiration of the Agreement for any reason or upon Waste Management's request, Supplier shall immediately cease handling Waste Management Data or portion of Waste Management Data specified by Waste Management, and shall return in a manner and format reasonably requested by Waste Management, or, if specifically directed by Waste Management, shall destroy in a manner required by Section 12 above, any or all such Waste Management Data in Supplier's possession, power or control, in whatever form, including, without limitation, all copies, fragments, excerpts, and any materials containing Waste Management Data, whether or not such Waste Management Data has been intermingled with Supplier's own information or materials. Upon Waste Management's instruction to destroy or return Waste Management Data, all copies of Waste Management Data shall be permanently removed from Supplier's, its agents', subcontractors' and third parties' systems, records, archives and backups and all subsequent use of such Waste Management Data by Supplier, its agents, subcontractors and third parties shall cease. Upon request, an officer of Supplier will certify to Waste Management that all forms of the requested Waste Management Data have been destroyed by Supplier.

24. Subject to any specific terms or conditions in the Agreement regarding the rendering of transition or termination assistance, at Waste Management's request, which request may be made (i) at any time the Agreement or any renewal thereof remains in effect and (ii) for a period of up to twelve (12) months following the effective termination or expiration of the Agreement, Supplier shall provide such reasonable termination or transition assistance as requested by Waste Management to (a) continue the Services without interruption or adverse effect and (a) facilitate the orderly transfer of all or any part of the Services to Waste Management or such third party as identified by Waste Management (collectively, "Termination Support"). Any Termination Support shall be provided in accordance with the Agreement, exclusive of any provisions therein regarding the term or renewal thereof. The obligations of Supplier under this Attachment shall continue for so long as Supplier continues to have access to, is in possession of or acquires Waste Management Data, even if all agreements between Supplier and Waste Management have expired or been terminated.

25. On the Effective Date of the Agreement, Supplier shall designate a management level employee as Supplier's primary security manager under the Agreement who shall be available to assist Waste Management twenty-four (24) hours a day, seven (7) days a week. Supplier's

primary security manager shall be responsible for managing and coordinating the performance of Supplier's obligations set forth in this Attachment.

26. Supplier shall indemnify, hold harmless, and defend Waste Management, Waste Management Entities, and its and their officers, directors, shareholders, employees, agents, successors, assigns, and subcontractors from and against any and all Claims and any and all threatened claims, losses, liabilities, damages, settlements, expenses and costs arising from, in connection with, or based on allegations of, in whole or in part, any of the following: (a) any violation of the requirements of this Attachment or the Data Protection Requirements; (b) any Breach; (c) any negligence or willful misconduct of Supplier, the Supplier Parties or any third party to whom Supplier provides access to Waste Management Data or systems, with respect to security or confidentiality of Waste Management Data; (d) remedial action taken by Waste Management as the result of a Breach; and (e) any other costs incurred by Waste Management with respect to Waste Management's rights in this Attachment. Except as otherwise provided herein, Supplier shall be fully responsible for, and shall pay, all costs and expenses incurred by Supplier or its personnel or agents with respect to the obligations imposed under this Attachment.

27. In the event that Supplier is unable to comply with the obligations stated in this Attachment, Supplier shall promptly notify Waste Management, and Waste Management shall then be entitled (at its option) to suspend the transfer of Waste Management Data, require Supplier to cease using relevant Waste Management Data and/or immediately terminate the Agreement.