Phoenix Marketing International Privacy Policy
Regarding
Data Collected from Employees

Phoenix Marketing International (PMI) is strongly committed to protecting the privacy of those who entrust us with their personal data. We will maintain this trust by protecting the privacy of personal data of our employees, as well as our employees' family members and beneficiaries.

This Policy applies to PMI and the PMI group of companies including all affiliated companies, divisions, branches, offices, subsidiaries and controlled affiliates (all of which are collectively referred to as "PMI", "we", or "our") and to all employees, independent contractors, and vendors of PMI.

As part of this commitment, PMI will comply with:

- The EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information
- The Health Insurance Portability and Accountability Act of 1996, as amended from time to time
- ("HIPPA"), with respect to PMI operations in the United States; and
- All other privacy laws, rules and regulations that apply to PMI in each location in which PMI has operations.

This policy describes:

How we collect and treat data the personal data of our employees and their families:

- The personal data that PMI typically collects and the sources that provide that data such as employees, employees' family members or dependents, beneficiaries or third-parties;
- How PMI typically uses or discloses personal data PMI collects;
- The employees and other business organizations that typically have access to the personal data that PMI collects;
- How PMI protects the personal data it collects; Rights to review and correct personal data;
- How to notify PMI about improper disclosure or use of personal data and the action PMI may take after determining that personal data has been improperly disclosed or used; and
- The circumstances under which employees will be given a choice to "opt out" or decline PMI's collection, use, or disclosure of personal data.

Nothing in this policy is intended to imply, nor will anything in this policy be deemed to create, any ownership interest or privacy right in any voice or data transmission over PMI voice or data networks. PMI retains ownership of, and, where consistent with applicable laws and regulations, the right to inspect, copy, retain, and intercept all electronic mail, voice mail, telephone conversations and other electronic communications created using or transmitted over PMI's voice or data networks or using or transmitted over PMI equipment. For further information on the use of PMI networks, please refer to PMI's Information Security Policy.

I. Definitions

A. "Business Contact Personal Data" ("BCD") means personal data that it is reasonably necessary to disclose for an employee to be contacted by those who have legitimate business needs to do so. BCD includes; name, job title, job function, office address, office telephone and fax numbers, business e-mail address and, where PMI pays for such services devices either directly or through reimbursement, cellular telephone number.

B. "Business Personal Data" ("BPD") means data relating to any identified or identifiable individual that is reasonably necessary to be disclosed or used (1) for an employee to perform his or her job functions effectively and efficiently; (2) for management to manage the work of the individual or to manage the individual's training, development or performance; (3) for the Company to administer compensation and benefit programs; or (4) that the Company is legally required to collect and disclose to governmental agencies (e.g. tax authorities or immigration authorities) in compliance with applicable laws and regulations. Examples of BPD include, but are not limited to, name, home address, home telephone number, national identification numbers such as social security or social insurance numbers, performance history, work assignment history, immigration data, health data required to administer benefit programs, date of birth, pay rate or salary, etc.

C. "Sensitive Personal Data" ("SPD") means all identified or identifiable personal data of a particularly sensitive nature, and usually, but not always, recognized as such in legislation or government regulation. SPD can include: racial or ethnic origin or health and medical information. Sensitive personal data includes protected health information as such term is defined in HIPAA. PMI collects, stores, uses, and discloses SPD only in order to carry out PMI's legal obligations as an employer including its role as a sponsor or provider of employee benefits.

II. Chief Privacy Officer

A. Chief Privacy Officer (CPO). PMI's Director of Human Resources is our Chief Privacy Officer. The CPO will conduct an assessment of PMI's compliance with this Employee Personal Data Privacy Policy at least annually. Upon completion of each assessment and implementation of any required changes to PMI's privacy practices, the CPO will certify the self-assessment report and verify PMI's compliance with this Policy in writing.

III. Notice of Personal Data Collected and Sources of Data Collection

A. Data Collection from Employees and Dependents/Family Members
Personal data is collected from individuals when they apply for employment with PMI, when they accept an offer of employment with PMI, enroll in PMI's benefit programs, or during the course of their employment with PMI. Employees may disclose personal data to PMI by updating their personal data through automated HRIS and benefits systems. Employees may also disclose personal data in non-automated systems through communications with supervisors and managers, with individuals in Human Resources, and with third-parties such as benefit vendors. PMI does receive personal data in connection with (i) pre-employment and other background checks in countries where these checks are conducted, (ii) enrollment for medical and other insurance benefits, and (iii) in certain cases, when employees or their dependents seek medical insurance or other PMI benefits.

B. Specific Data Examples.
PMI will collect personal data in a specific jurisdiction only as allowed by the laws and regulations applicable to that specific jurisdiction. In accordance with those local laws, personal data collected may include, but is not limited to, the following:

- Personal identification information such as name, date of birth, gender, national identification numbers (e.g. social insurance, social security, or tax payer numbers), driver's license number, passport number, etc.;
- Employment-related personal background information such as education (including schools attended, and dates of attendance, degrees or diplomas granted), training, work history (including names of employers, dates of employment, and compensation information), military and veteran status, and criminal history;
- Contact information such as home and office address, home, office and cellular telephone numbers, home and office e-mail address, etc.;
- Compensation information, such as wages or salary, commissions, bonuses, stock program information, pension and 401(k) plan account information, etc.;

Health and medical information as collected in the administration of health or other benefits including information regarding employees, family members or dependents and related individuals, etc.; and
Job-related information such as work history, experience, training courses, performance information, job or functional assignments, etc.

C. Data Sources.
Personal data is received or collected from (i) employees and their family members when employees apply for employment or benefits, (ii) service providers in connection with pre- employment background checks, and (iii) health, medical and other benefit providers in connection with the administration of PMI benefits programs.

IV. Notice of Disclosure and Use of Personal Data

A. Business Contact Data, Business Personal Data, and Sensitive Personal Data
PMI discloses BCD, BPD, and SPD in the following circumstances: (i) to PMI Employees who reasonably need to receive such personal data to perform their duties for PMI; (ii) PMI's benefits providers who reasonably need to receive such personal data to administer benefit programs covering PMI employees; (iii) PMI clients and prospective clients regarding employees who are providing, or are proposed to provide, services (except that sensitive personal data is not disclosed to clients or prospective clients);and (iv) under applicable law to governmental entities or in response to valid legal processes.

B. Specific Examples.
Specific examples of PMI's use or disclosures include:

- An employee's supervisor and management have a business need to know the employee's personal, background, contact, compensation, work history, experience, training, and performance information in connection with managing his or her duties for PMI.
- Employees in finance, human resources and legal may also need to receive personal information to prepare budgets, administer compensation or benefit programs, or to advise PMI on compliance with its legal obligations. Employees given access to personal data for these purposes will receive training on data protection as a condition of being provided data access. PMI may disclose Business Contact Personal Data to PMI employees and other individuals and organizations without any restriction on its further use or restriction by the recipient. Our policy is not to disclose employee home addresses or telephone numbers to PMI employees or other individuals or organizations without the employee's prior approval, except that PMI may disclose your home address and telephone number (i) to PMI supervisors and managers who have a business need to know, and (ii) in emergency and critical business situations to other PMI
- employees and emergency assistance vendors who need to contact employees. Personal data of employee family members or dependents may also be provided to PMI employees and
- emergency service vendors in similar circumstances.

Disclosure to Third-Parties.
Consistent with the Privacy Shield Principles, PMI may disclose BCD and BPD to PMI's agents that are outside firms and consultants (who will, in turn, disclose your personal data to their employees and consultants) who advise PMI on compensation matters or benefits programs or who administer such programs for PMI. PMI requires each of these agents, outside firms and consultants (other than licensed professionals, such as lawyers and doctors, who are subject to legally enforceable client confidentiality obligations) to sign a written confidentiality agreement that requires them to adequately protect data provided to them and prohibits them (and their employees and consultants) from disclosing or using your personal data in any way that is not necessary to perform the services they have been engaged to provide. This confidentiality agreement must be signed before PMI will disclose Business Personal Data. PMI may also disclose Business Contact Data and Business Personal Data of employees to customers and prospective customers where the employees whose data are disclosed are providing, or are proposed to provide, services to the third-party but only for purposes consistent with this Policy and subject to agreements requiring adequate protection and prohibiting further disclosure. Sensitive personal

data is not routinely disclosed to customers or prospective customers and will not be disclosed without your prior written consent.

PMI may be required to disclose Business Contact Data, Business Personal Data or Sensitive Personal Data under applicable law or in response to valid legal process. These disclosures would include responses to valid search warrants, subpoenas, court orders, or other official request from a government or regulatory authority or agency. PMI reserves the right to disclose information in order to satisfy its legal obligations. Furthermore, PMI may disclose Business Personal Data or Sensitive Personal Data to government or regulatory authorities or agencies if PMI has reason to believe that disclosure is required under applicable law (for example, if PMI discovers evidence of a crime or attempted crime). Disclosures may also be appropriate to protect PMI's legal rights (e.g. theft of trade secret case), when physical safety is believed to be at risk, or to notify family members or public or private disaster relief agencies of your location or condition.

PMI may disclose Business Personal Data or Sensitive Personal Data about an employee or his or her family to a group health plan where PMI is the sponsor of, or performs plan administration functions for, that group health plan, as specified in the relevant plan documents.

PMI does not disclose or sell Employees' personal data to any company or person for marketing purposes.

V. Choice

PMI will adhere to the Choice Principle of the Privacy Shield. PMI internally discloses and uses employee Business Personal Data in connection with the management of day-to-day operations, in business planning, in the management of legal proceedings, and for emergency response. Except in limited circumstances, such as those involving Sensitive Personal Data, an employee's consent to the disclosures and uses of that employee's personal data for the purposes described in this Policy will not be requested. PMI's CPO will make the ultimate determination whether or not a particular disclosure or use is described in this policy. If PMI develops a potential use or disclosure of personal data that is not described in this Policy, then PMI will notify employees of this new purpose for use or disclosure. PMI will offer employees a choice whether or not to allow PMI to use or disclose their personal data for that new purpose. In this situation, employee consent must be received in writing (or a legally equivalent electronic form) before PMI uses or discloses personal data for this new purpose.

VI. Onward Transfer

PMI will comply with the Onward Transfer Principle of the Privacy Shield including adherence to the Notice and Choice Principles for disclosure to non-agent third parties. PMI will ensure all data transfers comply with the data privacy requirements of the employee's home country and those of the country in which the data is stored or processed. PMI will ensure that transferred data is adequately protected from accidental disclosure and from theft or intentional disclosure or misuse. Where appropriate or when required by applicable laws, PMI will implement data transfer agreements to specify the applicable standards of protection for transferred data. PMI assumes liability in cases of onward transfers to third parties.

VII. Security

PMI applies physical, electronic, and procedural safeguards that we believe provide adequate protection of data and comply with applicable laws to guard personal data against loss, unauthorized access, destruction, misuse, modification, or improper disclosure. Business Contact Data, Business Personal Data, and Sensitive Personal Data are retained in PMI's human resources database, other systems or records (for example, Information Technology provisioning systems or directory servers) or in physical form. The human resources database and other PMI automated systems are maintained on computer equipment located in restricted access environments, both by PMI and Automatic Data Processing, Inc. In addition to physical security measures, PMI uses electronic security safeguards that protect against unauthorized access to restrict systems access to a limited number of employees whose duties require access to the information. Physical files are retained in restricted access environments or locked storage containers when not being used.

All employees whose job duties require access to Business Personal Data or Sensitive Personal Data are trained on their data protection obligations and on protective measures as a condition of being provided access to the data.

VIII. Data Integrity, Purpose Limitation and Access

PMI will not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual, for the extent of time that this information is kept. Individuals will have access to personal information about them that PMI holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

IX. Enforcement

PMI's Chief Privacy Officer will promptly review and investigate every allegation that this Policy has been violated by any employee, customer, outside firm, consultant, or other unauthorized party. As part of this review and investigation, the Chief Privacy Officer will review any relevant processes and procedures to determine whether changes are necessary to prevent a recurrence of any substantiated violation of this policy.

PMI will, at its sole discretion and in accordance with all applicable laws, take disciplinary action against any employee who violates this policy. The severity of the disciplinary action taken will vary based on factors considered relevant including:

- the sensitivity of the personal data disclosed or used in violation of this policy;
- the number of employees impacted by the violation of this policy;
- the duration of the improper disclosure or use;
- prior improper disclosure or use of personal data by that employee, and
- whether the violation was inadvertent, foreseeable, the result of negligence, or arose from a deliberate or reckless act.

Except where (i) the improper disclosure or use of personal data was inadvertent or the result of inadequate training, or (ii) the Chief Privacy Officer determines that the circumstances do not warrant such action for other reasons, appropriate disciplinary action will be taken in accordance with PMI's corrective action or disciplinary policies. Among other forms of action available, violations of this Policy

may result in a written warning, suspension without pay (to the extent permitted by applicable law) or termination of employment. In all cases, the Chief Privacy Officer shall determine whether additional training or process modifications are also required.

The Chief Privacy Officer will review any violation of this Policy by a customer, client, outside firm or consultant with a senior manager of such client, outside firm, or consultant to determine the appropriate corrective action. Unless the Chief Privacy Officer determines otherwise, appropriate disciplinary action with respect to an employee or consultant of a client, outside firm or consultant who violates this Policy should include actions similar to those that would occur if the employee or consultant were a PMI employee. In addition, the Chief Privacy Officer may recommend to the Executive Team whether the business relationship between PMI and the customer, client, outside firm or consultant should be terminated as a result of the violation.

The results of each investigation, including any disciplinary action recommended or taken, will be reported to the PMI's Executive Team, per established reporting procedures. Where PMI believes that the conduct may constitute a violation of any applicable law, rule or regulation, the conduct may be disclosed to appropriate law enforcement and regulatory authorities.

In addition to its internal investigative and resolution efforts, PMI will cooperate with the European Union Data Protection Authorities ("DPAs") in their efforts to investigate and resolve complaints brought under the Privacy Shield. PMI will comply with advice given by the DPAs, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Privacy Shield Principles. PMI is also subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) / the Department of Transportation. Under certain conditions, individuals may invoke binding arbitration using the measures and policies outlined in this document.

In compliance with the Privacy Shield Principles, PMI commits to resolve complaints about our collection or use of your personal information. EU individuals with inquiries or complaints regarding our Privacy Shield policy should first contact PMI at:

You may also mail a report to: Chief Privacy Officer
Phoenix Marketing International
6423 Montgomery Street
Suite 12
Rhinebeck, NY 12572

PMI has further committed to refer unresolved Privacy Shield complaints to eTrust, an alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please contact or visit eTrust for more information or to file a complaint. The services of eTrust are provided at no cost to you, and can be accessed at the following URL:

http://www.etrust.org/complaint/index.html

X. Country / Geographic Exceptions & Modifications

PMI reserves the right to change this Privacy Policy from time to time.

Should you have any questions or suggestions about our privacy practices, or wish to update or correct any personally identifiable information that you have chosen to provide to us, please contact the Human Resources department.

Should you wish to report a violation or suspected violation, you can contact any member of PMI management, any member of PMI human resources or PMI's legal team.

You may also mail a report to:
Chief Privacy Officer
Phoenix Marketing International
6423 Montgomery Street
Suite 12
Rhinebeck, NY 12572

Phoenix Marketing International Privacy Policy
Regarding
Information Collected Survey Respondents and Panel Members

Privacy Policy:
Phoenix Marketing International (PMI) is strongly committed to protecting the privacy of those who entrust us with their personal data during the course of our business operations. We will maintain this trust by protecting the privacy of personal data provided to us by survey respondents and panel members, whether disclosed directly to us by the individual or received from a third party.

Scope:
This Policy applies to PMI and the PMI group of companies including all affiliated companies, divisions, branches, offices, subsidiaries and controlled affiliates (all of which are collectively referred to as "PMI", "we", or "our") and to all employees, independent contractors, and vendors of PMI.

As part of this commitment, PMI will comply with:

- The EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information.
- The Health Insurance Portability and Accountability Act of 1996, as amended from time to time
- ("HIPAA"), with respect to PMI operations in the United States; and
- The Financial Privacy Requirements of the Gramm Leach-Bliley Financial Modernization Act of
- 1999; and
- All other privacy laws, rules and regulations that apply to PMI in each location in which PMI has operations.

Nothing in this policy is intended to imply, nor will anything in this policy be deemed to create, any ownership interest or privacy right in any voice or data transmission over PMI voice or data networks. PMI retains ownership of, and, where consistent with applicable laws and regulations, the right to inspect, copy, retain, and intercept all electronic mail, voice mail, telephone conversations and other electronic communications created using or transmitted over PMI's voice or data networks or using or transmitted over PMI equipment or that of its vendors.. For further information on the use of PMI networks, please refer to PMI's Information Security Policy.

Definitions:

"Panel" refers to a panel of U.S. households or individuals recruited by PMI or its vendors whose members have agreed to participate in telephone, mail or Internet-based Survey Research from time to time.

"Respondent" refers to a member of the public who is contacted and agrees to participate with PMI for the purpose of conducting Survey Research.

"Survey Research" refers to telephone surveys, mail surveys, Internet surveys, door to door surveys, ad hoc panels, continuous panels, mall intercepts, business-to-business surveys, focus groups, one-on-one executive interviews, media rating services, mystery shopping, employee surveys, and all other types of survey research.

"Personal Information" means information that individually or in combination could identify a specific individual. Examples include first and last name, home postal address or personal email address. Personal information does not include information that is lawfully obtained from publicly available

resources, or from federal, state, or local government records lawfully made available to the general public.

"**Demographic Information**" refers to characteristics (such as health issues or consumer habits), attributes and demographic information (such as age, income, gender) (collectively, "Demographic Information").

"**Operating Information**" refers to information other than personal and demographic information, gathered by PMI from respondents in the course of interfacing with respondents, including information about their interests, needs and attitudes as they relate to the subject of the market research study.

Privacy Principles:

Although privacy and data protection laws vary from country to country, most are based on the following privacy principles. Accordingly, to assure compliance with all applicable data protection laws and achieve consistency across the organization, PMI will adhere to the following privacy principles at least to the extent required by applicable law:

I. Notice

In all cases, PMI must inform respondents and panel members about

- the purposes for which it collects information about them how to contact us with any inquiries or complaints
- the types of third parties to which we discloses the information
- the choices and means the organization offers individuals for limiting its use and disclosure

This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to PMI or as soon thereafter as is practicable, but in any event before we use such information for a purpose other than that for which it was originally collected or discloses it to a third party

A. Notice of Personal Data Collected and Sources of Data Collection

When we contact a survey respondent or panel member, we will generally do so for one of the following purposes:

- To invite them to participate in survey research;
- To conduct a survey research interview with them;
- To validate answers they gave in a recent survey we conducted;
- To update and to ensure that our records of their personal information are correct.

Much more occasionally, we may contact a survey respondent or panel member for one of these other purposes:

- To notify them if they have won a sweepstakes we sponsored;
- To ask for them permission to use their personal information for a purpose that was not identified to them when we first collected their personal information.

Data Collection from Survey Respondents/Panel Members

Personal and Demographic Information: During the PMI recruitment process, PMI may collect personal information such as a respondent's name, email address, home address, names and ages of members of the respondents' and panel members' household ("Personal Information"). In addition, PMI frequently asks respondents and panel members for characteristics (such as health issues or consumer habits), attributes and demographic information (such as age, income, gender) (collectively, "Demographic Information").

The respondents and panel members are in control of the Personal Information they provide to PMI. We rely on them to update their Personal and Demographic information. They may:

- Ask for a copy of their Personal or Demographic Information
- Ask for Personal or Demographic Information to be updated or corrected
- Ask PMI to remove their Personal or Demographic records from PMI's records

When respondents and panel members make these requests, we will comply with their request in a reasonable timeframe.

Operating Information: PMI may, in the course of interfacing with respondents and panel members, gather other types of information from respondents and panel members ("Operating Information"). For example, PMI respondents and panel members may receive surveys from us which inquire about respondents and panel members' interests, needs and attitudes. PMI will receive the responses from these surveys. Similarly, if PMI offers other features, services or programs in which respondent explicitly agrees to participate, then PMI will receive information from those features, services or programs.

B. Notice of Disclosure and Use of Personal Data

Authorized Uses of PMI Data subject Information:

Personal and Demographic Information: Personal information, such as email addresses, may be used for each data subject who is 13 years of age or older, to communicate with respondents and panel members and household members, and to assist respondents and panel members with questions they may have about the PMI Panel. It may also be used for panel recruitment, contest entry processing or delivery of free gifts to members of the PMI panel. Personal information concerning location or address may also be used to ensure that our panel accurately represents the target population.

Respondents and panel members may be asked for Demographic Information in order to pre-qualify members or households for surveys that target specific groups. PMI also uses this information to ensure that our panel accurately represents our target population

PMI uses Personal Information and Demographic Information solely in the conduct of its research business. Personal Information or Demographic Information may be combined with information collected about respondents and panel members by PMI or third parties with respondents and panel members' express permission, with information that is collected about data subject from public records, or with information that PMI may acquire from third parties that have a legal right to provide such information to PMI.

Operating Information:
PMI uses operating information solely in the conduct of its research business. As is the case with Personal Information and Demographic Information, Operating Information may be combined with information collected about respondents and panel members by PMI or third parties with respondents and panel members' express permission, with information that is collected about data subject from public records, or with information that PMI may acquire from third parties that have a legal right to provide such information to PMI.

C. How PMI May Share Information:
Personal Information regarding respondents and panel members will never be shared with any third parties without the respondents and panel members' express permission, except that we may disclose a respondent's or panel member's information if we are required to do so by law, if we need to do so to protect someone's safety or our rights or property, or in order to comply with this policy or other policies that may be applicable. In addition, occasionally, PMI will share contact information such as name and address with third parties with whom we have partnered to provide specific services to PMI, or services on behalf of PMI, such as panel recruitment, contest entry processing or deliver of free gifts to PMI respondents and panel members. In each of these instances, a privacy agreement will be signed by these partners and they will be contractually obligated not to use any personally identifiable information except for the purpose of providing these services, unless the respondent or panel member enters into a relationship with them that would directly allow them to do so.

PMI collects and shares Demographic Information and Operating information with our research clients in an anonymous form. It is our policy to never share Personal Information of respondents and panel members with our clients, nor should our clients ever be able to identify respondents and panel members without the respondent's or panel member's express permission.

In addition to keeping survey responses confidential, PMI will never sell, share, rent or otherwise intentionally transfer respondents' or panel members' names, addresses, telephone numbers or e-mail addresses to our clients, other market research companies, direct marketing companies or anyone else.

PMI is an expanding business, and like other companies, we sometimes acquire or divest business units. As part of such transfers, we may convey the business assets of the particular business unit, including Personal Information, Demographic Information, or Operating Information of respondents and panel members.

D. Data Transfers:
Personal Information, Demographic Information and Operating Information will generally be stored in PMI's databases, or our vendors' databases, which are located in the United States. For easier processing of email communications, contests, sweepstakes, or other marketing purposes, however, Personal Information, Demographic Information and Operating Information may be sent, usually on a temporary basis, to countries outside the United States or the European Union. PMI data protection standards are the same, regardless of where the information is stored.

E. Children's Privacy:
PMI believes that it's especially important to protect children's privacy online and encourages parents and guardians to spend time online with their children to participate and monitor their Internet activity.

PMI will comply with the Children's Online Privacy Protection Act of 1998. We do not permit children who are under 13 years of age to become PMI respondents or panel members. We do not collect any Personal Information from children under 13 years of age. As part of the registration process for new Respondents and panel members we collect the names of each individual in the respondent's or panel member's household, which may include the names of children who are under 13 years of age. Occasionally we may send a survey to a respondent or panel member who is a parent or guardian of a child under the age of 13 that asks that respondent or panel member to have his or her child who is under 13 answer the survey. We take reasonable steps to ensure parental consent to such procedure by sending the survey to the parent or guardian's password protected email address. The information collected in response to such surveys is not combined with identifiable information about the child. In every case such survey will not collect Personal Information about the child.

If a respondent or panel member has provided us with Personal Information about a child in their household who is under the age of 13, and the parent or guardian of that child requests that we delete this information from our records, we will promptly comply with this request, and use reasonable efforts to delete the child's information from our databases.

II. Choice
PMI will adhere to the Choice Principle of the Privacy Shield as follows:

Opt Out:
PMI must offer individuals the opportunity to choose (opt out) whether and how personal information they provide is used or disclosed to third parties (where such use is incompatible with the purpose for which it was originally collected or with any other purpose disclosed to the individual in a notice). They must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise this option.

Opt In:
For sensitive information, such as medical and health information, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information concerning the sex life of the individual they must be given affirmative or explicit (opt in) choice.

III. Onward Transfer

PMI will comply with the Onward Transfer Principle of the Privacy Shield including adherence to the Notice and Choice. In a situation where we have not provided choice to the individual because a use is compatible with the purpose for which the data was originally collected or which was disclosed in a notice and we wish to transfer the data to a third party, we may do only upon first either ascertaining that the third party subscribes to the Privacy Shield principles or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Privacy Shield principles.

PMI will ensure all data transfers comply with the data privacy requirements of the employee's home country and those of the country in which the data is stored or processed. PMI will ensure that transferred data is adequately protected from accidental disclosure and from theft or intentional disclosure or misuse. Where appropriate or when required by applicable laws, PMI will implement data transfer agreements to specify the applicable standards of protection for transferred data. PMI assumes liability in cases of onward transfers to third parties.

IV. Data Security and Responsibility

PMI is committed to keeping the data provided to us secure and will take reasonable precautions to protect Personal Information from loss, misuse or alteration. Vendors, contractors or partners of PMI who have access to personal information in connection with providing services for PMI are contractually required to keep the information confidential and are not permitted to use this information for any other purpose than to carry out the services they are performing for PMI.

PMI safeguards Personal Information, Demographic Information and Operating Information from unauthorized access. Most Operating Information is maintained in databases that are separate from those containing Personal Information and Demographic Information. Only authorized PMI employees or agents carrying out permitted business functions are allowed to access these databases. In addition, each employee of PMI is required to sign a confidentiality agreement requiring him or her to keep confidential all Personal Information of Respondents and panel members.

PMI applies physical, electronic, and procedural safeguards that we believe provide adequate protection of data and comply with applicable laws to guard personal data against loss, unauthorized access, destruction, misuse, modification, or improper disclosure. Collected Data is retained in PMI's database, other systems or records (for example, Information Technology provisioning systems or directory servers) or in physical form. All employees whose job duties require access to Personal Data or Sensitive Personal Data are trained on their data protection obligations and on protective measures as a condition of being provided access to the data.

V. Data Access and Integrity

PMI recognizes the need for accuracy and completeness of all personal data it collects or receives. Consistent with these principles, PMI may only process personal information relevant to the purposes for which it has been gathered. To the extent necessary for those purposes, employees should take reasonable steps to ensure that data is accurate, complete, and current.

VI. Enforcement

PMI's Director of Human Resources is our Chief Privacy Officer. The CPO will conduct an assessment of PMI's compliance with this Employee Personal Data Privacy Policy at least annually. Upon completion of each assessment and implementation of any required changes to PMI's privacy practices, the CPO will certify the self-assessment report and verify PMI's compliance with this Policy in writing.

PMI's Chief Privacy Officer will promptly review and investigate every allegation that this Policy has been violated by any employee, customer, outside firm, consultant, or other unauthorized party. As part of this review and investigation, the Chief Privacy Officer will review any relevant processes and procedures to determine whether changes are necessary to prevent a recurrence of any substantiated violation of this policy.

PMI will, at its sole discretion and in accordance with all applicable laws, take disciplinary action against any employee who violates this policy. The severity of the disciplinary action taken will vary based on factors considered relevant including:

- the sensitivity of the personal data disclosed or used in violation of this policy;
- the number of employees impacted by the violation of this policy;
- the duration of the improper disclosure or use;
- prior improper disclosure or use of personal data by that employee, and
- whether the violation was inadvertent, foreseeable, the result of negligence, or arose from a deliberate or reckless act.

Except where (i) the improper disclosure or use of personal data was inadvertent or the result of inadequate training, or (ii) the Chief Privacy Officer determines that the circumstances do not warrant

such action for other reasons, appropriate disciplinary action will be taken in accordance with PMI's corrective action or disciplinary policies. Among other forms of action available, violations of this Policy may result in suspension without pay (to the extent permitted by applicable law) or termination of employment. In all cases, the Chief Privacy Officer shall determine whether additional training or process modifications are also required.

The Chief Privacy Officer will review any violation of this Policy by a customer, client, outside firm or consultant with a senior manager of such client, outside firm, or consultant to determine the appropriate corrective action. Unless the Chief Privacy Officer determines otherwise, appropriate disciplinary action with respect to an employee or consultant of a client, outside firm or consultant who violates this Policy should include actions similar to those that would occur if the employee or consultant were a PMI employee. In addition, the Chief Privacy Officer may recommend to the Executive Team whether the business relationship between PMI and the customer, client, outside firm or consultant should be terminated as a result of the violation.

The results of each investigation, including any disciplinary action recommended or taken, will be reported to the PMI's Executive Team and Board of Directors, per established reporting procedures. Where PMI believes that the conduct may constitute a violation of any applicable law, rule or regulation, the conduct may be disclosed to appropriate law enforcement and regulatory authorities.

In addition to its internal investigative and resolution efforts, PMI will cooperate with the European Union Data Protection Authorities ("DPAs") in their efforts to investigate and resolve complaints brought under the Privacy Shield. PMI will comply with advice given by the DPAs, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Privacy Shield Principles.

VII. Country / Geographic Exceptions & Modifications

Any PMI business unit at the country, geography, or location level may modify this policy to provide greater protections than contained herein where legally required to do so. However, no PMI business unit may modify this Policy to provide less protection than contained herein.

PMI reserves the right to change this Privacy Policy from time to time.

Should you have any questions or suggestions about our privacy practices or this policy, please contact the Chief Privacy Officer at Human.Resources@PhoenixMI.com.

Should you wish to report a violation or suspected violation, you can contact any member of PMI management, any member of PMI human resources or PMI's legal team.

You may also mail a report to:
Chief Privacy Officer
Phoenix Marketing International
6423 Montgomery Street
Suite 12
Rhinebeck, NY 12572