5) Please provide the total number of individuals' records, including those of employees and third party's, that contain any of the information from question 3) above that the applicant is responsible for keeping secure

☒ 1 – 5,000 ☐ 5,001 – 10,000 ☐ 10,001 – 25,000

☐ 25,001 – 50,000 ☐ 50,001+:

Please provide approximate number: _____

6) Does the Applicant currently comply with the following standards/regulations?

Standard/Regulation	Yes	No	N/A	
Payment Card Industry – Data Security Standard (PCI-DSS)	☒	☐	☐	N/A *if Applicant does not accept credit or debit cards for payment)*
Level of PCI Compliance: _____				
HIPAA/ HITECH	☐	☐	☒	N/A: *if Applicant is not defined as a "covered entity" or "business associate" under HIPAA*
Graham-Leach-Bliley (GLB)	☐	☐	☒	N/A: *if Applicant is not a financial services entity as defined under GLB*
California CIVIL CODE SECTION 1790-1790.4 (Cal. SB 1386)	☐	☐	☐	*California Song-Beverly Credit Card Act*
MA Law 201 CMR 17	☐	☐	☐	*Massachusetts' Data Protection Law*
FACTA, FCRA	☐	☐	☐	*Fair and Accurate Credit Transactions Act*
DMCA Safe Harbor Provision	☐	☐	☐	*Digital Millennium Copyright Act of 1998*
State privacy protection laws	☐	☐	☐	

7) Approximate % of operations that are outsourced: 0%
Please indicate the operation(s) outsourced and the name of the third party contractor:

Network Security Service Provider	☐ Yes	☐ No	
Data Storage/Back-up/Recovery	☐ Yes	☐ No	
Credit Card Transaction Processing	☒ Yes	☐ No	*First Data*
Website Hosting	☐ Yes	☐ No	
Application Service Provider (ASP)	☐ Yes	☐ No	
Finance and/or HR Functions	☒ Yes	☐ No	*People Strategy Consulting, LLC*

Please provide any service contracts with the above third party contractors.

D. NETWORK SECURITY

1) Does the Applicant physically protect access to dedicated computer rooms and/or servers? ☒ Yes ☐ No

2) Within the last three years, have you ever had an improper network security breach by an internal employee?

☒ Never ☐ 1-3 times ☐ more than 3 ☐ more than 10

Describe the incident and any actions taken to prevent future occurrences: _____

---

3) Does the Applicant utilize remote shutdown of employee laptops? ☐ Yes ☐ No

4) Does the Applicant permit the use of thumb drives or external memory drives by employees? ☐ Yes ☐ No

If yes, does the Applicant use detection technology to monitor or detect the use of thumb drives/external memory drives access? ☐ Yes ☐ No

5) Does the Applicant conduct criminal background checks on all new employees who have access to Nonpublic Personal Information (NPI) or Company Confidential Information (CCI)? ☐ Yes ☐ No

6) Does the Applicant restrict employee and contractor's access to Nonpublic Personal Information on a need-to-know basis? ☒ Yes ☐ No

7) Are there formal processes to revoke network privileges immediately following an employee's or contractor's termination or resignation? ☒ Yes ☐ No

8) Does the Applicant conduct annual training with employees that addresses data privacy and IT security controls and responsibilities? ☒ Yes ☐ No

9) Is there an e-mail detection system in place to monitor for unauthorized access to an email server or download of personal information or large file download? ☒ Yes ☐ No

10) Does the Applicant conduct a network security process and practices audit for third party vendors? ☒ Yes ☐ No

11) Does the Applicant have written contracts in place, with all third party contractors who have access to the Applicant's Computer System? ☐ Yes ☐ No

If yes, do the contracts specifically address information security, privacy and the protection of Nonpublic Personal Information and Company Confidential Information with standards at least to the level of the applicants (including the use of encryption?) ☐ Yes ☐ No

12) Does the Applicant contractually require all third party contractors and consultants that may host or access data to:

    a) certify that they meet equivalent security and privacy standards as the insured? ☐ Yes ☐ No

    b) validate that they have not had any previous privacy or security breach? ☐ Yes ☐ No

13) Does the Applicant conduct penetration testing of their computer network(s)? ☐ Yes ☐ No

14) Does the Applicant enforce a software update process as new releases or improvements become available: ☐ Yes ☐ No

If yes, are critical patches installed within 15 days of release? ☐ Yes ☐ No

15) Does the Applicant maintain procedures regarding the destruction of data residing on systems or devices prior to their disposal, recycling, resale or refurbishing? ☒ Yes ☐ No

16) Please indicate the security readiness of the Applicant's organization below.

Security Controls:		
Compliant with ISO 27001 IT Security Standards	☐Yes	☐No
Anti-virus software	☐Yes	☐No
Network monitoring and prevention technologies, including wireless devices	☐Yes	☐No
Firewall in place	☐Yes	☐No
Utilize and regularly review results of automated database monitoring tools which continually monitor, record, analyze, alerts including automatic shutdown when data access irregularity detected.	☐Yes	☐No
Redundant network available for back up, and date lasted tested for continuity. Date of last test:	☐Yes	☐No
Data Loss Prevention Technology (DLP)	☐Yes	☐No
Conduct periodic intrusion detection, penetration or vulnerability testing	☐Yes	☐No

17) Does the Applicant have a documented network security breach incident response plan? ☒ Yes ☐ No

18) Does the Applicant encrypt Nonpublic Personal Information (NPI) or Company Confidential Information (CCI) in the following environments?

The Applicant's computer system	☐Yes	☐No	☐ N/A, if Applicant does not maintain their own Computer System (i.e. service provider utilized for all network functions)
When sending emails containing Nonpublic Personal Information over public networks	☐Yes	☐No	☐ N/A, if Applicant does not send emails containing NPI

On laptops	☐Yes	☐No	☐ N/A, if Applicant does not store NPI on laptops
On mobile storage media, including thumb drives, memory sticks, storage tapes, "smartphones" and other mobile devices	☐Yes	☐No	☐ N/A, if Applicant does not store NPI on mobile devices
When collected by the Applicant and hosted by a third party (including back-ups)	☐Yes	☐No	☐ N/A, if Applicant does not store NPI on mobile devices

19) Does the Applicant require third party subcontractors who have access to the Applicant's Computer System to carry:

a) Errors & Omissions insurance ☒ Yes ☐No

b) Network Security and Data Privacy insurance coverage? ☐ Yes ☐No

E. MEDIA AND INTERNET CONTENT

1) Describe the function of the Applicant's websites (check all that apply):

☒ Basic Informational: information and content about the Applicant's products and services

☒ Content aggregation: content from third party sources but approved and filtered by the Applicant

☒ Interactive Web 2.0: visitors and/or employees can interact with the website by posting content.

☐ E-Commerce: for the buying /selling of goods and services

☐ Transactional: financial transactions other than "e-commerce"

2) Is the Applicant pursuing any social networking initiatives, including maintaining a presence on a social networking site? ☐Yes ☐No

If so, please provide a description. _____

3) Does the Applicant's website(s) allow for third parties or employees to post their own comments and content via a chatroom or bulletin board included in your site? ☒Yes ☐No

If yes, please check all that apply:

All content is reviewed by authorized person prior to publication ☒Yes ☐No

Blog or site content monitoring technology is used to detect abuses of site "terms & conditions" ☒Yes ☐No

4) Does the Applicant allow customers to rate/rank/give an opinion on competitor's product/service? ☐Yes ☐No

5) Does the Applicant's website include operating or maintaining a blog? ☒Yes ☐No

If so, is the blog content reviewed prior to posting? ☒Yes ☐No

6) Does the Applicant have a formal "take-down" policy to remove any infringing, libelous or otherwise controversial materials from their website? ☒Yes ☐No

7) Does the Applicant utilize in-house or outside counsel to review all website content prior to posting? ☒Yes ☐No

8) Is there a review process to screen the Applicant's online content/ marketing/ mass email for the following? Please check all that apply:

☒	Libel	☒	Trademark and Copyright Infringement	☒	Privacy Violations
☒	Defamation	☒	Domain name infringement	☒	Opt-in/Opt-out status

12) Does the Applicant regularly screen your web site and web site posting for potential copyright or trademark infringements? ☒Yes ☐No

If yes, how: _____

13) Does the Applicant use software to help manage your Intellectual Property applications? ☐Yes ☐No

14) Select the Intellectual Property (IP) protections the Applicant employs in business operations:

IP Controls		
IP protection within Employee Agreements	☐Yes	☐No
IP protection within Non-Disclosure Agreements (NDA) with all third parties	☐Yes	☐No
Trade secret agreements with third parties where applicable	☐Yes	☐No
Prior Act Searches by a legal professional (internal or external)	☐Yes	☐No
Acquisition of all necessary IP rights via licenses, releases, or consents	☐Yes	☐No
Take down policy on web site for notifications of IP related complaints	☐Yes	☐No
Acquire written permission of sites you link to or frame	☐Yes	☐No