

Please attach a copy of your most recently audited annual financial statement.

Are significant changes in the nature or size of the Applicant's business anticipated over the next twelve (12) months? Or have there been any such changes within the past twelve (12) months? Yes No

If yes, please explain:

Has the Applicant within the past twelve (12) months completed or agreed to, or does it contemplate entering into within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed? Yes No

If yes, please explain:

I. MANAGEMENT OF PRIVACY EXPOSURES

- 1. Has the Applicant designated a Chief Privacy Officer? Yes No
If no, please indicate what position (if any) is responsible for privacy issues:
- 2. Does the Applicant have a written corporate-wide privacy policy? Yes No
If yes, please attach a copy of the privacy policy to this application.
- 3. Is the Applicant in compliance with its privacy policy? Yes No
If no, please provide details regarding such non-compliance:
- 4. Does the Applicant accept credit cards for goods sold or services rendered? Yes No
If yes:
 - A. Please state the Applicant's approximate percentage of revenues from credit card transactions in the most recent twelve (12) months: %
 - B. Is the Applicant compliant with applicable data security standards issued by financial institutions the Applicant transacts business with (e.g. PCI standards)? Yes No
If the Applicant is not compliant with applicable data security standards, please describe the current status of any compliance work and the estimated date of completion:
- 5. Does the Applicant restrict employee access to personally identifiable on a business-need to know basis? Yes No
- 6. Does the Applicant require third parties with which it shares personally identifiable information or confidential information to indemnify the Applicant for legal liability arising out of the release of such information due to the fault or negligence of the third party? Yes No
- 7. Has the Applicant implemented an identity theft prevention program (aka FTC "Red Flags" program)? Yes No
- 8. If the Applicant is in the healthcare industry, does the Applicant host, operate, or manage a Healthcare Information Exchange on which other organizations may store personal health information? Yes No

II. COMPUTER SYSTEMS CONTROLS

- 1. Has the Applicant designated a Chief Security Officer as respects computer systems? Yes No
If no, please indicate what position is responsible for computer security:
- 2. Does the Applicant publish and distribute written computer and information systems policies and procedures to its employees? Yes No
- 3. Does the Applicant conduct training for every employee user of the information systems in security issues and procedures for its computer systems? Yes No
- 4. Does the Applicant have :

A. a disaster recovery plan?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
B. a business continuity plan?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
C. an incident response plan for network intrusions and virus incidents?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
How often are such plans tested?		
5. Does the Applicant have a program in place to test or audit security controls on an annual or more frequent basis?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
If yes, please summarize the scope of such audits and/or tests:		
6. Does the Applicant terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
7. Is all valuable/sensitive data backed-up by the Applicant on a daily basis?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
If no, please describe exceptions:		
8. Is at least one complete back-up file generation stored and secured off-site separate from the Applicant's main operations in a restricted area?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
If no, describe the procedure used by the Applicant, if any, to store or secure copies of valuable/sensitive data off-site?		
9. Does the Applicant have and enforce policies concerning when internal and external communication should be encrypted?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
A. Are users able to store data to the hard drive of portable computers or portable media devices such as USB drives?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
B. Does the Applicant encrypt data stored on laptop computers and portable media?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
C. Please describe any additional controls the Applicant has implemented to protect data stored on portable devices:		
10. What format does the Applicant utilize for backing up and storage of computer system data?		
<input type="checkbox"/> Tape or other media <input type="checkbox"/> Online backup service <input type="checkbox"/> Other:		
A. Are tapes or other portable media containing backup materials encrypted?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
B. Are tapes or other portable media stored offsite using secured transportation and secured storage facilities?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
1) If stored offsite, are transportation logs maintained?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If stored onsite, please describe physical security controls:		
11. Does the Applicant enforce a software update process including installation of software "patches"?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If Yes, are critical patches installed within thirty (30) days of release?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
12. Please describe your network infrastructure:		
Primary vendor:	Anti-virus	Firewall
Other significant vendor:	ISP	Intrusion Detection
13. How often are virus signatures updated? <input type="checkbox"/> Automatic Updates <input type="checkbox"/> Weekly <input type="checkbox"/> Monthly <input type="checkbox"/> Other		
14. Does the Applicant require computer service providers who may have access to confidential information or personally identifiable information to demonstrate adequate security policies and procedures?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
A. Are computer service providers required by contract to indemnify the Applicant for harm arising from a breach of the provider's security?	<input type="checkbox"/> Yes	<input type="checkbox"/> No