QSR
Quaker Special Risk

DataBreach

APPLICATION FOR DATA BREACH AND PRIVACY LIABILITY, DATA BREACH LOSS TO INSURED AND ELECTRONIC MEDIA LIABILITY INSURANCE

Notice: The liability coverage(s) for which application is made: (1) applies only to “Claims” first made during the “Policy Period” and reported to the Company during the “Policy Period” or within sixty days after the expiration of the “Policy Period”, unless the Extended Reporting Period is exercised; and (2) the limits of liability shall be reduced by “Claim Expenses” and “Claim Expenses” shall be applied against the deductible.

Please read the policy carefully.

If space is insufficient to answer any question fully, attach a separate sheet.

If response is none, state NONE.

I. GENERAL INFORMATION

1. (a) Full Name of Applicant: ______________________________

(b) Principal business premise address: ______________________________
(Street) (County)

____
(City) (State) (Zip)

(c) Phone Number: ______________________________

(d) Date formed/organized (MM/DD/YYYY): ______________________________

(e) Business is a: [ ] corporation [ ] partnership [ ] individual [ ] other ____________

(f) Website(s):______________________________

2. Describe in detail the Applicant’s business operations:

____

____

____

3. Does the Applicant use internal staff or an outside service provider to manage its IT systems? ....[ ] Internal [ ] Outside

(a) If outside service provider, provide name of organization: ______________________________

4. How many individual offices/locations does the Applicant have? ___________

II. OPERATIONS AND BUSINESS FUNCTIONS

1. Applicant's annual gross revenues:

		Total (including E- Commerce)	E-Commerce Only
(a)	Estimated annual gross revenues for the coming year:	$_____________	$____________
(b)	For the past twelve (12) months:	$_____________	$____________

2. Applicant’s annual transactions:

		Total	E-Commerce	Credit/Debit Card
(a)	Estimated annual transactions for the coming year:	__________	________%	________%
(b)	For the past twelve (12) months:	__________	________%	________%

3. Number of employees including principals and independent contractors:
Full-time _______ Part-time ______ Seasonal/Temporary ______ Independent Contractors ______ Total _______

4. Number of individual devices the Applicant has deployed:
Servers ________ Desktops _________ Laptops _________ Mobile Phones/Devices_________

5. Does the Applicant handle sensitive data for any of the following:

		Transmit/Receive	Store
(a)	Credit Cards/Debit Cards?	[ ] Yes [ ] No....................	[ ] Yes [ ] No
(b)	Financial/Banking Information?	[ ] Yes [ ] No....................	[ ] Yes [ ] No
(c)	Medical Information (PHI)?	[ ] Yes [ ] No....................	[ ] Yes [ ] No
(d)	Social Security Numbers or National Identification Numbers?	[ ] Yes [ ] No....................	[ ] Yes [ ] No
(e)	Other (specify) ____	[ ] Yes [ ] No....................	[ ] Yes [ ] No

6. Indicate the number of sensitive data records the Applicant stores currently:

[ ] None [ ] 1 to 50,000 [ ] 50,001 to 100,000 [ ] 100,001 to 150,000

[ ] 150,001 or more; estimate number of records: _________

7. Does the Applicant use an outside vendor or service provider to process or store sensitive information?
.... [ ] Yes [ ] No
(a) If Yes, provide name of organization and details: ____

III. SECURITY INCIDENT AND LOSS HISTORY

1. Has the Applicant at any time during the past three (3) years had any incidents, claims or suits involving unauthorized access, intrusion, breach, compromise or misuse of the Applicant's network, including embezzlement, fraud, theft of proprietary information, theft or loss of laptops, denial of service, electronic vandalism or sabotage, computer virus or other incident?.. [ ] Yes [ ] No
If Yes, attach full details including a description of each incident, claim or suit and the cause, internal costs, cost to third parties, recovery time and steps taken to mitigate future exposure.

2. Is the Applicant or any of its principals, partners, officers, directors, trustees, managers, managing members, or employees, its predecessors, subsidiaries, affiliates or any other persons or organizations proposed for this insurance aware of any fact, circumstance, situation or incident related to the Applicant's network which might give rise to a loss or a claim? .... [ ] Yes [ ] No
(a) If Yes, provide full details: ____
____

3. Has any application for similar insurance made on behalf of the Applicant, its predecessors, subsidiaries, affiliates, and/or for any other person(s) or organization(s) proposed for this insurance ever been declined, cancelled or nonrenewed?.. [ ] Yes [ ] No
(a) If Yes, provide full details: ____
____

4. Has the Applicant at any time during the past three (3) years had any incidents, claims or suits involving the following and/or is the Applicant aware of any fact, circumstance, situation or incident related to the following which might give rise to a claim:
(a) Infringement of copyright, trademark, trade dress, rights of privacy or rights of publicity? .... [ ] Yes [ ] No
(b) Libel, slander or other form of disparagement, arising out the Applicant's web site or other electronic media?... [ ] Yes [ ] No
If Yes, to either of the above provide full details: ____
____

IV. IT SYSTEM SECURITY

By attachment provide explanation of any No response.

If an outside service provider is used to manage the Applicant's IT System, please consult with such outside service provider when completing these questions.

A. Risk Management & Security Policy

1. Does the Applicant have:
(a) an Executive Risk Committee that provides information security and data oversight?.................. [ ] Yes [ ] No
(b) written information security policies and procedures that are reviewed annually? .... [ ] Yes [ ] No

2. Does the Applicant perform risk assessments prior to conducting business with external software companies or service providers?... [ ] Yes [ ] No

3. How often does the Applicant conduct risk assessments?..........[ ] None [ ] Quarterly [ ] Bi-annually [ ] Annually

B. Information Security Organization and Asset Management

1. Does the Applicant have a dedicated senior manager responsible for Information Security and Privacy? .... [ ] Yes [ ] No
   (a) If Yes, provide Name and Title:
   (b) If No,
   (i) Who is responsible?
   (ii) Is the person responsible an: [ ] Internal Resource [ ] External Resource

2. Does the Applicant have a written program to manage the lifecycle of its IT assets and sensitive data? .... [ ] Yes [ ] No

C. Human Resources and Physical Security

1. Does the Applicant perform background checks on all employees and contractors with access to portions of its network that contain sensitive data?...................... [ ] Yes [ ] No

2. How often does the Applicant conduct information security awareness training?
   [ ] Never [ ] Monthly [ ] Quarterly [ ] Bi-Annually [ ] Annually

3. Does the Applicant have a process to delete systems access after employee termination? .... [ ] Yes ≤ 48 hours [ ] Yes > 48 hours [ ] No

4. Is access to equipment, such as servers, workstations and storage media including paper records, containing sensitive information physically protected?...................... [ ] Yes [ ] No
   (a) If Yes, how is it physically controlled? [ ] Areas open to employees only [ ] Role based access controls

D. Communications and Operations Management

1. Does the Applicant have a written security patch management process implemented?...................... [ ] Yes [ ] No
   (a) If Yes, how are security patch notifications from its major systems vendors handled?
   [ ] No automatic notice
   [ ] Automatic notice (where available) and implemented in more than 30 days
   [ ] Automatic notice (where available) implemented in 30 days or less

2. Does the Applicant have anti-virus, anti-spyware and anti-malware software installed?...................... [ ] Yes [ ] No
   (a) If Yes, check all that apply:
   [ ] On all desktop and laptop computers with automatic updates
   [ ] On all server computers with automatic updates
   [ ] Scanning of all incoming email
   [ ] Scanning of all web browsing

3. Does the Applicant implement firewalls and other security appliances between the Internet and sensitive data? .... [ ] Yes [ ] No

4. Does the Applicant have standards in place to ensure that all devices on its network are securely configured? .... [ ] Yes [ ] No
   (a) If Yes, which of the following applies:
   [ ] Change default administrative passwords
   [ ] Implement appropriate security settings and standards
   [ ] Remove unneeded services

5. Are security alerts from an intrusion detection or intrusion prevention system (IDS/IPS) continuously monitored and are the latest IDS/IPS signatures installed regularly? .... [ ] Yes [ ] No

6. Does the Applicant store sensitive information on any of the following media? If Yes, is it encrypted?

		Sensitive Data	Encrypted
(a)	Laptop hard drives?......................	[ ] Yes [ ] No......................	[ ] Yes [ ] No
(b)	PDA's / other mobile devices?......................	[ ] Yes [ ] No......................	[ ] Yes [ ] No
(c)	Flash drives or other portable storage devices?......................	[ ] Yes [ ] No......................	[ ] Yes [ ] No
(d)	Back-up tapes?......................	[ ] Yes [ ] No......................	[ ] Yes [ ] No
(e)	Internet connected web servers?......................	[ ] Yes [ ] No......................	[ ] Yes [ ] No
(f)	Databases, audit logs, files on servers?......................	[ ] Yes [ ] No......................	[ ] Yes [ ] No
(g)	Email?......................	[ ] Yes [ ] No......................	[ ] Yes [ ] No

7. Does the Applicant ensure sensitive data is permanently removed (e.g., degaussing, overwriting with 1's and 0's, physical destruction but not merely deleting) from hard drives and other storage media before equipment is discarded or sold and from paper records prior to disposal? .... [ ] Yes [ ] No

(a) If Yes, how is data permanently removed?
[ ] Paper records with sensitive data shredded
[ ] Data permanently removed before equipment sold or discarded

E. Access Control

1. How does the Applicant limit access to its IT Systems:
[ ] No controls or use shared log on ID's
[ ] Unique user ID's
[ ] Unique user ID's and role based access to sensitive data

2. Does the Applicant secure remote access to its IT systems? .... [ ] Yes [ ] No
(a) If Yes, how does the Applicant secure remote access?
[ ] ID/password only [ ] VPN or equivalent [ ] VPN or equivalent with two factor authentication

3. Does the Applicant require minimum security standards (anti-virus, firewall, etc.) for all computers used to access its network remotely? .... [ ] Yes [ ] No

4. Does the Applicant have written security policies and procedures for mobile devices, including personal devices, if they are connected to the Applicant's network? .... [ ] Yes [ ] No

5. Does the Applicant have wireless networks deployed? .... [ ] Yes [ ] No
If Yes,
(a) Are all wireless access points to the Applicant's network encrypted with WPA/WPA2 or more recent standard (e.g., not unencrypted or using WEP standard)? .... [ ] Yes [ ] No
(b) Is there a firewall between all wireless access points and the parts of the Applicant's network on which sensitive information is stored? .... [ ] Yes [ ] No

F. Information Systems Management and Development

1. Does the Applicant have a Systems Development Lifecycle (SDLC) in place for specifying, building/acquiring, testing, implementing and maintaining its IT systems with information security built into the process?...................... .... [ ] Yes [ ] No

2. Is a vulnerability scan or penetration test performed on all Internet-facing applications and systems before they go into production and at least quarterly thereafter?.. [ ] Yes [ ] No

3. Are all sessions where sensitive data is entered encrypted with a Secure Socket Layer (SSL)? .... [ ] Yes [ ] No

4. Does the Applicant implement secure coding standards based on best practices to defend against known security issues (Cross Site Scripting, SQL Injection, etc.) for all applications that the Applicant develops in-house?.. [ ] N/A [ ] Yes [ ] No

G. Incident Management and Compliance

1. Does the Applicant have a written incident management response plan?... [ ] Yes [ ] No

2. Is the Applicant certified as complying with the following security requirements:
(a) Payment Card Industry (PCI/DSS)? ....[ ] N/A [ ] Yes [ ] No [ ] In Progress - Scheduled Date: __________
(i) If Yes, provide the name of the individual or outside organization which certified the Applicant and the date of the last PCI audit.____
(b) HIPAA/HITECH?.................................[ ] N/A [ ] Yes [ ] No [ ] In Progress - Scheduled Date: __________
(c) GLBA? ....[ ] N/A [ ] Yes [ ] No [ ] In Progress - Scheduled Date: __________
(d) Red Flags Rules? ....[ ] N/A [ ] Yes [ ] No [ ] In Progress - Scheduled Date: __________
(e) Sarbanes-Oxley? ....[ ] N/A [ ] Yes [ ] No [ ] In Progress - Scheduled Date: __________

3. Are annual or more frequent internal/external audit reviews performed on the Applicant's network?...... [ ] Yes [ ] No
(a) If Yes, attach a copy of the last examination/audit of the Applicant's network operations, security and internal control procedures.

H. Data Breach Loss to Insured Coverage

Check if coverage not requested. [ ]

1. Are alternative facilities available in the event of a shutdown/failure of the Applicant's network?............ [ ] Yes [ ] No

2. Does the Applicant have written procedures for routine backups and maintain proof of backups? .... [ ] Yes [ ] No

3. Are key data and software code stored:
(a) on redundant storage device? .... [ ] Yes [ ] No
(b) at secured offsite storage? .... [ ] Yes [ ] No

I. Electronic Media Liability Coverage

Check if coverage not requested. [ ]

1. Does the Applicant conduct prior review of any content, including (if applicable), blogs, for copyright infringement, trademark infringement, libel or slander, violation of rights of privacy or publicity?........... [ ] Yes [ ] No
   (a) If Yes, who is responsible for reviews (internal counsel, outside counsel, etc.)? ____________________________

2. Does the Applicant have take down procedure to comply with DMCA safe harbor provisions if hosting content posted by third parties on their servers or web site? .... [ ] NA [ ] Yes [ ] No

3. Does the Applicant obtain clear rights to intellectual property (IP) supplied by third parties if such IP is displayed on their web site?... [ ] Yes [ ] No

4. Does the Applicant use the names or likeness of any celebrities or other public figures on their web site? .... [ ] Yes [ ] No

V. PRIOR AND OTHER INSURANCE

1. List current and prior Cyber Liability or Cyber Security Insurance for each of the last three (3) years:
   If None, check here [ ]

Insurance Company	Limits of Liability	Deductible	Premium	Inception-Expiration Dates (MM/DD/YYYY)	Retroactive/ Prior Acts Date

2. Provide the following insurance information:

	Insurer	Limit	Deductible	Expiration Date
A. General Liability:				
B. Professional Liability:				

NOTICE TO THE APPLICANT - PLEASE READ CAREFULLY

No fact, circumstance, situation or incident indicating the probability of a claim, loss or action for which coverage may be afforded by the proposed insurance is now known by any person(s) or entity(ies) proposed for this insurance other than that which is disclosed in this application. It is agreed by all concerned that if there be knowledge of any such fact, circumstance, situation or incident any claim subsequently emanating therefrom shall be excluded from coverage under the proposed insurance.

This application, information submitted with this application and all previous applications and material changes thereto of which the underwriting manager, Company and/or affiliates thereof receives notice is on file with the underwriting manager, Company and/or affiliates thereof and is considered physically attached to and part of the policy if issued. The underwriting manager, Company and/or affiliates thereof will have relied upon this application and all such attachments in issuing the policy.

For the purpose of this application, the undersigned authorized agent of the person(s) and entity(ies) proposed for this insurance declares that to the best of his/her knowledge and belief, after reasonable inquiry, the statements in this application and in any attachments, are true and complete. The underwriting manager, Company and/or affiliates thereof are authorized to make any inquiry in connection with this application. Signing this application does not bind the Company to provide or the Applicant to purchase the insurance.

If the information in this application or any attachment materially changes between the date this application is signed and the effective date of the policy, the Applicant will promptly notify the underwriting manager, Company and/or affiliates thereof, who may modify or withdraw any outstanding quotation or agreement to bind coverage.

The undersigned declares that the person(s) and entity(ies) proposed for this insurance understand that the liability coverage(s) for which this application is made apply(ies):

(i) Only to “Claims” first made during the “Policy Period” and reported to the Company during the “Policy Period” or within sixty days after the expiration date of the “Policy Period,” unless the extended reporting period is exercised. If the extended reporting period is exercised, the policy shall also apply to “Claims” first made during the extended reporting period and reported to the Company during the extended reporting period or within sixty days after the expiration of the extended reporting period;

(ii) The limits of liability contained in the policy shall be reduced, and may be completely exhausted by “Claim Expenses” and, in such event, the Company will not be liable for “Claim Expenses” or the amount of any judgment or settlement to the extent that such costs exceed the limits of liability in the policy; and

(iii) “Claim Expenses” shall be applied against the “Deductible”.

WARRANTY

I/We warrant to the Company, that I/We understand and accept the notice stated above and that the information contained herein is true and that it shall be the basis of the policy and deemed incorporated therein, should the Company evidence its acceptance of this application by issuance of a policy. I/We authorize the release of claim information from any prior insurer to the underwriting manager, Company and/or affiliates thereof.

Note: This application is signed by the undersigned authorized agent of the Applicant(s) on behalf of the Applicant(s) and its, owners, partners, directors, officers and employees.

Must be signed by director, executive officer, partner or equivalent within 60 days of the proposed effective date.

Name of Applicant

Title

Signature of Applicant

Date

Notice to Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and subjects the person to criminal and civil penalties.