FailSafe® Cyber / Information Risk Supplement Application

Expense and Claims Made Disclosure
This application is for a claims first made policy. Please contact Your agent or broker if You have any questions. The policy, if issued, applies only to claims when the wrongful act occurs on or after the retroactive date and before the end of the policy period, and the claim is first made against any of You during the policy period. An extended reporting period may also be available.

Covered claim expenses and damages within the retention amount must be paid by You and do not reduce Limits of Liability. Covered claim expenses and damages above the retention amount are payable under the policy, and may reduce, and may completely exhaust the limits of liability. We shall not be liable for claims expenses or damages after exhaustion of the applicable Limit of Liability.

Whenever used in this Application, the term "Applicant" shall mean the entity proposed as the **Named Insured** and any subsidiaries thereof, and the respective directors, officers, trustees, and governors of all such entities.

GENERAL INFORMATION			
Name of Applicant:			
Mailing Address:		State:	
City:		Zip Code:	

ASSET IDENTIFICATION AND MANAGEMENT

1. Does the Applicant have a Chief Privacy Officer or equivalent position? ☐ Yes ☐ No
   If not, are there any other positions that are responsible for privacy related issues? ☐ Yes ☐ No
   Position title: _____
   % of time spent on privacy related issues: _____%
2. Does the Applicant have a Chief Information Security Officer or equivalent position? ☐ Yes ☐ No
   If not, are there any other positions that are responsible for security related issues? ☐ Yes ☐ No
   Position title: _____
   % of time spent on security related issues: _____%
3. Has the Applicant identified and inventoried systems and physical devices (including laptops and mobile devices) within the Applicant's information system? ☐ Yes ☐ No
4. Does the Applicant collect, process, control, use, or share sensitive information? ☐ Yes ☐ No
   If yes, please check all that apply and provide approximate number of records.

☐ Social Security Numbers:	_____	☐ Healthcare Records:	_____
☐ Payment Card Information:	_____	☐ Medical Identification Information:	_____
☐ Drivers' License Numbers:	_____	☐ Credit Rating Information:	_____
☐ Financial Account Numbers:	_____	☐ User Names and Passwords:	_____
☐ Other Government ID Numbers:	_____	☐ Third Party Confidential Data:	_____
☐ Biometric Data:	_____	☐ Other: _____	_____

5. Has the Applicant conducted a risk assessment of the assets identified in Question 4? ☐ Yes ☐ No
   a. Does the risk assessment include an asset classification system to identify assets that require heightened controls? (e.g. public, confidential, critical) ☐ Yes ☐ No
   b. Has the Applicant applied risk-appropriate controls (administrative, physical, or technical) to each class of identified assets based on the risk assessment? ☐ Yes ☐ No

6. Does the Applicant have a written information security policy?	☐ Yes	☐ No
a. Updated within the last: ☐ 120 Days ☐ 180 Days ☐ Year ☐ Never Updated		
b. Is the Applicant in compliance with its written information security policy?	☐ Yes	☐ No
7. Does the Applicant have an attorney-reviewed privacy policy that governs the collection, use, sharing, and retention of personal information?	☐ Yes	☐ No
a. Updated within the last: ☐ 120 Days ☐ 180 Days ☐ Year ☐ Never Updated		
b. Is the Applicant in compliance with its privacy policy?	☐ Yes	☐ No
8. Does the Applicant provide privacy notices to consumers on its website and mobile applications?	☐ Yes	☐ No
a. Have the privacy notices been reviewed by an attorney?	☐ Yes	☐ No
b. Are the Applicant's business practices consistent with its privacy notices?	☐ Yes	☐ No
9. Does the Applicant regularly assess its privacy and security policies for compliance with applicable standards and regulations? (If yes, check all that apply)	☐ Yes	☐ No
☐ PCI DSS (version: _____) ☐ Graham-Leach-Bliley Act		
☐ HIPAA/HITECH ☐ Identity Theft Red Flags Rule under FACTA		
☐ Other: _____		
10. Does the Applicant have and enforce a data retention policy?	☐ Yes	☐ No
a. Does the Applicant regularly and properly destroy sensitive data no longer necessary for business purposes?	☐ Yes	☐ No
b. Does the Applicant have a process for proper destruction of digital media and non-digital information in compliance with applicable regulations?	☐ Yes	☐ No

ASSET SECURITY AND PROTECTION		
1. Does the Applicant require approvals to create, disable, or modify information system accounts, including privileged and vendor accounts?	☐ Yes	☐ No
2. Does the Applicant limit access to information systems, including on mobile devices, by the business need to know and role of users, including employees and vendors?	☐ Yes	☐ No
3. Does the Applicant require complex passwords to access Applicant's networks, applications, and user accounts?	☐ Yes	☐ No
4. How often do users and vendors have to change passwords to access Applicant's network environment, applications, or user accounts?		
☐ At least every 90 days ☐ At least every 120 days ☐ At least every 180 days		
☐ 180 days or more ☐ No requirements to change passwords		
5. Does the Applicant limit the number of attempts to access a password protected account?	☐ Yes	☐ No
6. Does the Applicant deploy multifactor authentication for customers, clients, employees, and vendors to access Applicant's networks, applications, and user accounts?	☐ Yes	☐ No
7. Does the Applicant implement policies and controls regarding the number of concurrent sessions and session lock or termination?	☐ Yes	☐ No
8. Does the Applicant allow remote access to its network by employees or vendors?	☐ Yes	☐ No
• Does the Applicant restrict remote access to its network by employees and vendors to Virtual Private Networks?	☐ Yes	☐ No
9. Does the Applicant maintain physical access audit logs to server rooms, media storage areas, and data and communication centers?	☐ Yes	☐ No

10. Does the Applicant segment its network to protect sensitive data? ☐ Yes ☐ No
    a. Does the Applicant have information flow control policies? (e.g. firewalls that specify information transfer rules between connected systems) ☐ Yes ☐ No
    b. Does the Applicant have a policy and process for restricting transfers of sensitive information within its network? ☐ Yes ☐ No

11. Does the Applicant conduct background investigations of its new hires and require execution of appropriate access or non-disclosure agreements? ☐ Yes ☐ No

12. Does the Applicant conduct training for all employees, including privileged users (network administrators, information systems managers, etc.) regarding their privacy and security responsibilities and the Applicant's privacy, security, and use policies? ☐ Yes ☐ No
    a. Is the training provided at least on an annual basis to all employees? ☐ Yes ☐ No
    b. Does the Applicant record employee participation for every training session conducted? ☐ Yes ☐ No

13. Does the Applicant revoke network privileges within 2 business days following an employee's or contractor's termination or resignation? ☐ Yes ☐ No

14. Does the Applicant use encryption to protect sensitive information and its devices? ☐ Yes ☐ No
    a. Does the Applicant have an encryption key management policy, which includes encryption key rotation? ☐ Yes ☐ No
    b. Please indicate where the Applicant utilizes encryption (check all that apply):

    ☐ data transmitted over external networks
    ☐ data transmitted over its network
    ☐ data at rest
    ☐ desktops
    ☐ mobile devices, including laptops
    ☐ data processed, stored, or managed via cloud services
    ☐ removable storage media (including backup tapes)
    ☐ other: _____

15. Protection against Malicious Code:
    a. Does the Applicant deploy commercial grade boundary protection tools, including firewalls? ☐ Yes ☐ No
    b. Does the Applicant deploy commercial grade anti-virus/malware applications, which are updated and released to all devices within 24 hours? ☐ Yes ☐ No
    c. Is the anti-malware application configured to continuously scan or to perform periodic scans of the information system? ☐ Yes ☐ No
    d. Is the anti-malware application configured to scan files from external sources? ☐ Yes ☐ No
    e. How timely are security patches applied as they become available?
    ☐ Within 30 Days ☐ Within 90 Days ☐ Within 180 Days ☐ >180 Days

16. Does the Applicant have a policy that requires new or updated products, systems, databases, and software to be tested, and assessed for privacy and security issues? ☐ Yes ☐ No

17. Does the Applicant perform annual assessments for its physical and network security policies and procedures? (e.g. penetration testing by outside vendors) ☐ Yes ☐ No

18. Does the Applicant utilize data loss prevention tools to identify and monitor sensitive data and to prevent unauthorized transmissions of sensitive data? ☐ Yes ☐ No

19. Does the Applicant utilize software or hardware that is no longer supported or has been identified as end-of-life support by the software or hardware vendor? ☐ Yes ☐ No
    Please identify such software and hardware and outline any plans for remediation:

VENDOR MANAGEMENT

1. Approximately % of operations that are outsourced: _____%

   Please indicated the operation(s) outsourced and the name of the third party vendor(s):

   ☐ Network Security Service Provider: _____
   ☐ Data Storage/Back-up/Recovery: _____
   ☐ Systems Development and Maintenance: _____
   ☐ Payment Card Processing: _____
   ☐ Payment Applications: _____
   ☐ Point of Sale Devices: _____
   ☐ Payroll Services: _____
   ☐ Website Hosting: _____
   ☐ Other: _____

2. Does the Applicant utilize Cloud services? ☐ Yes ☐ No

   ☐ Infrastructure as a Service (IAAS) Provider: _____
   ☐ Platform as a Services (PAAS) Provider: _____
   ☐ Software as a Services (SAAS) Provider: _____

   a. Does the Applicant store, process, or otherwise manage Nonpublic Personal Information (NPI) or corporate confidential information through Cloud services? ☐ Yes ☐ No
   b. Does the Applicant have the ability to generate a unique encryption key? ☐ Yes ☐ No
   c. Does the Applicant regularly rotate its encryption keys? ☐ Yes ☐ No
   d. Does the Applicant have the right to audit system and application logs or network security controls of the cloud provider? ☐ Yes ☐ No
   e. Is Applicant's data segregated by physical segmentation (private or hybrid cloud)? ☐ Yes ☐ No
   f. Is Applicant's data segregated by network segmentation? ☐ Yes ☐ No
   g. Is Applicant's data segregated by application segmentation? ☐ Yes ☐ No

3. Does the Applicant have a vendor risk assessment program that has been approved by management? ☐ Yes ☐ No

4. Does the Applicant require written contracts for all third party vendors that have access to the Applicant's Computer System or sensitive information? ☐ Yes ☐ No

   If yes, do the contracts:

   a. specify privacy and security requirements and responsibilities? ☐ Yes ☐ No
   b. require the vendor to defend and indemnify the Applicant for liability arising from any compromise of the information due to the negligence of the vendor? ☐ Yes ☐ No
   c. require vendors' compliance with applicable privacy and security regulations? ☐ Yes ☐ No

5. Does the Applicant require vendors that have access to Applicant's Computer System or sensitive information to carry Data Privacy and Network Security insurance coverage? ☐ Yes ☐ No

6. Does the Applicant have a policy requiring an annual audit of the privacy and security practices of vendors to ensure compliance with applicable regulations and requirements? ☐ Yes ☐ No

   - If yes, is the Applicant in compliance with its policy for auditing the privacy and security practices of its vendors? ☐ Yes ☐ No

NETWORK MONITORING AND INTRUSION DETECTION

1. Are there positions within the Applicant organization dedicated to monitoring and detecting malicious network activity to ensure accountability? ☐ Yes ☐ No
   Position title: _____
   % of time spent on network monitoring issues: _____%
2. Does the Applicant establish, monitor and manage baselines for network operations and expected data flows for users and systems? ☐ Yes ☐ No
3. Does the Applicant review network activity against previously established baseline activity for unusual or abnormal activity? ☐ Yes ☐ No
4. Does the Applicant use intrusion detection or prevention systems, or network monitoring software to monitor network intrusions or unauthorized network activity? ☐ Yes ☐ No
5. Does the Applicant use security information and event management (SIEM) software to analyze and manage network events? ☐ Yes ☐ No
6. Log Generation, Analysis, Storage, and Monitoring
   a. Does the Applicant generate and collect logs related to network security, e.g. system logs, network logs and security application logs? ☐ Yes ☐ No
   b. Does the Applicant archive logs on a regular basis as part of standard operations? ☐ Yes ☐ No
   c. Does the Applicant have policies and procedures for managing and reviewing logs for unusual network activity or indicators of potential compromise? ☐ Yes ☐ No
   d. Does the Applicant conduct regular audits to confirm logging standards and guidelines are being followed? ☐ Yes ☐ No

INCIDENT RESPONSE PLANS

1. Does the Applicant have a written incident response plan related to a privacy or network security event? ☐ Yes ☐ No
   a. Does the incident response plan designate roles and responsibilities within the organization during the incident response? ☐ Yes ☐ No
   b. Does the Applicant train all employees regarding its incident response plan? ☐ Yes ☐ No
   c. Are employees (re)trained at least every year? ☐ Yes ☐ No
   d. Has the Applicant tested its incident response plan within the last 12 months? ☐ Yes ☐ No
   e. Has the Applicant updated its incident response plan within the last 36 months? ☐ Yes ☐ No
2. Does the Applicant track and document privacy and information system security events? ☐ Yes ☐ No

DISASTER RECOVERY PLANS

1. When did the Applicant last test its written business continuity and disaster recovery plans for an IT related event?
   ☐ <1 Year ago ☐ < 3 Years ago ☐ > 3 Years ago ☐ Never ☐ Applicant has no plans
2. Is there a position responsible for the development, maintenance, and testing of the above plans? Position title: _____ ☐ Yes ☐ No
3. How long would it take to restore the Applicant's operations after a network attack or unplanned system outage?
   ☐ 0-12 Hours ☐ 12-24 Hours ☐ 24-48 Hours ☐ More than 48 Hours ☐ Unknown
4. Does the Applicant backup system-level and user level information and data? ☐ Yes ☐ No
   a. Are backup tapes stored securely in an alternative site and properly purged after the retention period? ☐ Yes ☐ No
   b. How often does the Applicant backup system-level and user level information?
      ☐ Daily ☐ Weekly ☐ Monthly ☐ Never
5. Does the Applicant have an alternate storage site that maintains duplicate copies of information and data in the event that the primary site becomes unavailable? ☐ Yes ☐ No

6. Does the Applicant maintain an alternate processing site to maintain business function in the event that the primary site becomes unavailable?	☐ Yes	☐ No
7. Does the Applicant employ tools and controls to limit the effect of denial of service attacks? (e.g. utilizing boundary protection devices; creating sufficient capacity and service redundancies; managing network and storage capacities)	☐ Yes	☐ No

MEDIA / CONTENT / INTELLECTUAL PROPERTY

1. Does the Applicant have policies and procedures for editing or removing infringing or offensive content from its websites, social media platforms, or any other media or materials published or distributed by or on behalf of the Applicant?	☐ Yes	☐ No

2. Describe the activity or planned activity (next 12 months) on the Applicant's websites: (Check all that apply)

- ☐ provides information and content about the Applicant's products and services
- ☐ displays content aggregated from third party sources
- ☐ allows posting of content by visitors and/or employees on the website (e.g. forums, boards, chatrooms)
- ☐ manages forum or listing for the buying /selling of goods and services
- ☐ engages in financial transactions (payment card or virtual currency transactions)
- ☐ provides legal, financial, technology, health or medical advice
- ☐ has files for download
- ☐ provides gambling or adult entertainment services
- ☐ links or embeds content from media or networking sites (e.g. YouTube, Hulu, LinkedIn)

3. Does the Applicant manage or maintain a presence on any social media platforms?	☐ Yes	☐ No
a. Does the Applicant have a formal social media policy that has been approved by management?	☐ Yes	☐ No
b. Does the Applicant require employees to acknowledge receipt of the Applicant's social media policy?	☐ Yes	☐ No
c. Does the Applicant train employees regarding its social media policy?	☐ Yes	☐ No
d. Does the Applicant review content posted on its social media platforms for legal and regulatory issues?	☐ Yes	☐ No
4. Does the Applicant tailor, target, or market its websites, media, products, or services to children?	☐ Yes	☐ No
a. Does the Applicant collect data about children who use its websites or other internet services?	☐ Yes	☐ No
b. Does the Applicant have a process for obtaining appropriate consent prior to collection, use, or sharing of that data in compliance with applicable regulations?	☐ Yes	☐ No
5. Does the Applicant have written policies and procedures for clearing and protecting intellectual property rights for content displayed or disseminated on its internet media platforms, including websites, e-mail marketing, mobile apps, or social media?	☐ Yes	☐ No
a. Does the Applicant acquire all necessary rights, licenses, releases, and consent for its internet media content?	☐ Yes	☐ No
b. Does the Applicant acquire written permission from sites to which it links?	☐ Yes	☐ No
c. Does the Applicant protect intellectual property rights within employee and third party contractor agreements?	☐ Yes	☐ No
d. Does the Applicant regularly protect its intellectual property rights through nondisclosure agreements?	☐ Yes	☐ No
e. Does the Applicant screen all trademarks used by the Applicant for infringement prior to first use?	☐ Yes	☐ No

f. Please indicate whether the Applicant screens internet content, including postings and submissions by visitors, for the following:

- ☐ Copyright and trademark infringement
- ☐ Defamation
- ☐ Domain name infringement
- ☐ Privacy violations

ADDITIONAL APPLICATION MATERIALS

At the discretion of the Insurer, and as is relevant to the requested coverage(s), the following materials may be required.

- The most recent fiscal year-end financial statements;
- Any specific claim information related to prior losses;
- Explanations to all questions that require additional clarification;
- The latest edition of the Applicant's privacy policy and/or notice;
- The latest edition of the Applicant's written information security policy;
- A copy of service agreements used with third parties providing services or platforms to/for the Applicant.

IT IS UNDERSTOOD AND AGREED THAT ANY REPRIMAND, DISCIPLINARY OR CRIMINAL ACTIONS; LITIGATION, CLAIM, ARBITRATION, CIVIL, CRIMINAL, ADMINISTRATIVE OR REGULATORY ACTION OR PROCEEDING; OR KNOWLEDGE OR INFORMATION, ANY CLAIM OR ACTION FOR, BASED UPON, ARISING FROM OR IN ANY WAY RELATED THERETO IS EXCLUDED FROM THIS PROPOSED COVERAGE. THE INFORMATION PROVIDED IN THIS APPLICATION IS FOR UNDERWRITING PURPOSES ONLY AND DOES NOT CONSTITUTE NOTICE TO THE COMPANY OF A CLAIM OR POTENTIAL CLAIM UNDER ANY POLICY. IF YOU INTEND TO NOTICE A CLAIM OR POTENTIAL CLAIM FOR POSSIBLE COVERAGE, PLEASE COMPLY WITH THE NOTICE OF CLAIM CONDITIONS/PROVISIONS FOUND IN YOUR POLICY

The Undersigned declares that the person(s) and entity(ies) proposed for this insurance understands that:

- With respect to Liability Coverages, the **Policy** shall apply only to **Claims** made during the **Policy Period** or Extended Reporting Period (if applicable);
- The limit of liability contained in the **Policy** shall be reduced, and may be completely exhausted, by **Defense Expenses**, and, in such event, the Insurer shall not be liable for **Defense Expenses** or for the amount of any judgment or settlement to the extent that such cost exceeds the limit of liability in the **Policy**; and
- **Defense Expenses** that are incurred shall be applied against the retention amount.

FRAUD WARNING STATEMENTS

ATTENTION ALABAMA, ARKANSAS, DISTRICT OF COLUMBIA, MARYLAND, RHODE ISLAND AND WEST VIRGINIA APPLICANTS: ANY PERSON WHO KNOWINGLY (OR WILLFULLY IN MARYLAND) PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR KNOWINGLY (OR WILLFULLY IN MARYLAND) PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON.

ATTENTION COLORADO APPLICANTS: IT IS UNLAWFUL TO KNOWINGLY PROVIDE FALSE, INCOMPLETE, OR MISLEADING FACTS OR INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES, DENIAL OF INSURANCE, AND CIVIL DAMAGES. ANY INSURANCE COMPANY OR AGENT OF AN INSURANCE COMPANY WHO KNOWINGLY PROVIDES FALSE, INCOMPLETE, OR MISLEADING FACTS OR INFORMATION TO A POLICY HOLDER OR CLAIMANT FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE POLICY HOLDER OR CLAIMANT WITH REGARD TO A SETTLEMENT OR AWARD PAYABLE FROM INSURANCE PROCEEDS SHALL BE REPORTED TO THE COLORADO DIVISION OF INSURANCE WITHIN THE DEPARTMENT OF REGULATORY AGENCIES.

ATTENTION FLORIDA APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO INJURE, DEFRAUD OR DECEIVE ANY INSURER FILES A STATEMENT OF CLAIM OR AN APPLICATION CONTAINING ANY FALSE, INCOMPLETE, OR MISLEADING INFORMATION IS GUILTY OF A FELONY OF THE THIRD DEGREE.

ATTENTION KANSAS APPLICANTS: INSURANCE FRAUD IS A CRIMINAL OFFENSE IN KANSAS. A " FRAUDULENT INSURANCE ACT " MEANS AN ACT COMMITTED BY ANY PERSON WHO, KNOWINGLY AND WITH INTENT TO DEFRAUD, PRESENTS, CAUSES TO BE PRESENTED OR PREPARES WITH KNOWLEDGE OR BELIEF THAT IT WILL BE PRESENTED TO OR BY AN INSURER, PURPORTED INSURER, BROKER OR ANY AGENT THEREOF, ANY WRITTEN ELECTRONIC, ELECTRONIC IMPULSE, FACSIMILE, MAGNETIC, ORAL, OR TELEPHONIC COMMUNICATION OR STATEMENT AS PART OF, OR IN SUPPORT OF, AN APPLICATION FOR THE ISSUANCE OF, OR THE RATING OF AN INSURANCE POLICY FOR PERSONAL OR COMMERCIAL INSURANCE, OR A CLAIM FOR PAYMENT OR OTHER BENEFIT PURSUANT TO AN INSURANCE POLICY FOR COMMERCIAL OR PERSONAL INSURANCE WHICH SUCH PERSON KNOWS TO CONTAIN MATERIALLY FALSE INFORMATION CONCERNING ANY FACT MATERIAL THERETO; OR CONCEALS, FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO.

ATTENTION KENTUCKY, OHIO AND PENNSYLVANIA 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 SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES.

ATTENTION LOUISIANA, MAINE, TENNESSEE, VIRGINIA AND WASHINGTON APPLICANTS: IT IS A CRIME TO KNOWINGLY PROVIDE FALSE, INCOMPLETE OR MISLEADING INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES OR A DENIAL OF INSURANCE BENEFITS.

ATTENTION NEW MEXICO APPLICANTS: ANY PERSON WHO KNOWINGLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR KNOWINGLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO CIVIL FINES AND CRIMINAL PENALTIES.

ATTENTION NEW HAMPSHIRE AND NEW JERSEY APPLICANTS: ANY PERSON WHO INCLUDES ANY FALSE OR MISLEADING INFORMATION TO THE BEST OF HER/HIS KNOWLEDGE ON AN APPLICATION FOR AN INSURANCE POLICY IS SUBJECT TO CRIMINAL AND CIVIL PENALTIES.

ATTENTION OKLAHOMA APPLICANTS: WARNING, ANY PERSON WHO KNOWINGLY, AND WITH INTENT TO INJURE, DEFRAUD OR DECEIVE ANY INSURER, MAKES ANY CLAIM FOR THE PROCEEDS OF AN INSURANCE POLICY CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY.

ATTENTION OREGON APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD OR SOLICIT ANOTHER TO DEFRAUD AN INSURER: (1) BY SUBMITTING AN APPLICATION OR; (2) FILING A CLAIM CONTAINING A FALSE STATEMENT AS TO ANY MATERIAL FACT MAY BE VIOLATING STATE LAW.

ATTENTION NEW YORK 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 SHALL ALSO BE SUBJECT TO A CIVIL PENALTY NOT TO EXCEED FIVE THOUSAND DOLLARS AND THE STATED VALUE OF THE CLAIM FOR EACH SUCH VIOLATION.

THE UNDERSIGNED AUTHORIZED OFFICER OF THE APPLICANT DECLARES AND ACKNOWLEDGES THAT:

- THE POLICY CONTAINS A DEFENSE WITHIN LIMITS PROVISION WHICH MEANS THAT DEFENSE COSTS WILL REDUCE THE LIMIT OF LIABILITY AND MAY EXHAUST IT COMPLETELY AND SHOULD THAT OCCUR, THE INSURED SHALL BE LIABLE FOR ANY FURTHER LOSS, INCLUDING DEFENSE COSTS. IN ADDITION, DEFENSE COSTS ARE APPLIED AGAINST THE RETENTION.
- THE STATEMENTS SET FORTH HEREIN ARE TRUE AND COMPLETE[1]. THE UNDERSIGNED AUTHORIZED OFFICER AGREES THAT IF THE INFORMATION SUPPLIED ON THIS APPLICATION CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, THE UNDERSIGNED WILL, IN ORDER FOR THE INFORMATION TO BE TRUE AND COMPLETE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE INSURER OF SUCH CHANGES AND THE INSURER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS, AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE[2]**.** THE "EFFECTIVE DATE" IS THE DATE THE COVERAGE IS BOUND OR THE FIRST DAY OF THE POLICY PERIOD, WHICHEVER IS LATER. SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE INSURER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THIS APPLICATION SHALL BE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED AND IT WILL BE DEEMED ATTACHED TO AND BECOME A PART OF THE POLICY[3]. ALL WRITTEN STATEMENTS AND MATERIALS FURNISHED TO THE INSURER IN CONJUNCTION WITH THIS APPLICATION ARE HEREBY INCORPORATED BY REFERENCE INTO THIS APPLICATION AND MADE A PART HEREOF.

Applicable to risks FL, IA & NH

Applicant Signature and Date (Month/Day/Year)	Agent Name:
	Agent License Number (FL & NH Only)
Applicant Name and Title (print)	Agent Address
Name of Entity and Phone Number	Agent Signature and Date (FL & NH Only)

Application must be signed and dated by an owner, officer or partner.

1- In New Hampshire the truth and completeness shall be to the best of her/his knowledge.
2- In Maine this sentence ends at the word "quotations."
3- The application shall actually attach in the following states: North Carolina