THE MECHANIC GROUP,INC.
ONE BLUE HILL PLAZA, SUITE 530, PEARL RIVER, NY 10965
TEL - (845) 735-0700 FAX - (845)735-8383

PRIVACY//403 v2
PRIVACY LIABILITY AND NETWORK RISK INSURANCE
INSURANCE APPLICATION

THIS IS AN APPLICATION FOR A PRIVACY LIABILITY AND NETWORK RISK INSURANCE POLICY.

SUBJECT TO ITS TERMS, THE PROPOSED POLICY PROVIDES COVERAGE FOR CLAIMS FIRST MADE DURING THE POLICY PERIOD OR EXTENDED REPORTING PERIOD, IF APPLICABLE. THE APPLICABLE LIMITS OF INSURANCE AVAILABLE TO PAY DAMAGES OR SETTLEMENTS WILL BE REDUCED AND MAY BE EXHAUSTED BY THE PAYMENT OF DEFENSE EXPENSES.

- **This Application must be completed in full.**
- **If additional space is required for a response, include such response in an attachment to this Application, clearly identifying the question for which a response is being provided.**
- **Whenever used in this Application, the terms "Applicant," "You" or "Your Company" shall mean the organization proposed as the Named Insured and any Subsidiaries thereof, and their respective directors, officers, trustees, governors and employees.**
- **We treat all Applications as confidential.**

1. COVERAGE REQUESTED

(a) Indicate which coverages are being requested by Applicant:

- ☐ Privacy Liability
- ☐ Network Security Liability
- ☐ Media & Intellectual Property Liability
- ☐ First Party Business Interruption Coverage

LIMIT REQUESTED: ☐

DEDUCTIBLE REQUESTED: ☐

(b) Insurance Information:

Does the Applicant currently have the following insurance coverage in place?

Privacy Liability	Yes ☐	No ☐
Network Security Liability	Yes ☐	No ☐
Media / Intellectual Property Liability	Yes ☐	No ☐
First Party Business Interruption Coverage	Yes ☐	No ☐

If "Yes" to any of the above, please provide the following information for each policy:

Carrier:	☐	Limit:	☐
Deductible:	☐	Premium:	☐
Retro Date:	☐	Expiration Date:	☐

2. GENERAL INFORMATION

(a) Applicant's Name:

(b) Principal Address:
Street:
City: State: Zip Code:

(c) Year Established:

(d) Number of Employees:

(e) Website Addresses:
If any of these websites have a password protected or member/subscriber area, please provide temporary passwords and ID's lasting no longer than two weeks from the date of this Application.

(f) Provide the following information.

Use Fiscal Year basis	Prior Year	Current Year	Next Year (est.)
Total Revenue ($'s)			

(g) Describe the Applicant's primary business operations:

(h) In addition check any of the following that describes the Applicant's operations:
- ☐ Healthcare Organization
- ☐ Financial Institution
- ☐ Retailer
- ☐ E-Commerce site
- ☐ University
- ☐ Credit/Debit Card Processor
- ☐ Other:

(i) Does the Applicant organization have a Parent Entity? Yes ☐ No ☐

If "Yes," provide details:

(j) Is the Applicant currently or in the next 12 months planning to be involved in, or has the Applicant in the past 24 months been involved in, a merger, acquisition or divestment (whether or not such transaction was actually completed)? Yes ☐ No ☐

If "Yes," please detail:

(k) Please provide the contact information for the Applicant's Risk Manager. If none, please state.
Name:
Phone:
Email Address:

3. PERSONALLY IDENTIFIABLE INFORMATION (PII)

(a) Please quantify (by number of individual records) the Personally Identifiable Information (PII)* the Applicant currently stores, processes or transacts within its Network. (If unable to provide an exact number, please provide a best estimate, and describe the methodology for arriving at this estimate.) Number ☐

Methodology: ☐

* *Personally Identifiable Information is information from which an individual may be uniquely and reliably identified, including, but not limited to an individual's name, address, telephone number, in combination with their social security number, account relationships, account numbers, passwords, PIN numbers, credit or debit card numbers, biometric information, Nonpublic Personal Information as defined by the Gramm-Leach Bliley Act of 1999, or Personal Health Information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").*

(b) Describe how the Applicant stores PII within its Network. ☐

(c) Complete the following table with respect to how the Applicant protects PII stored in the following technology assets within its Network:

Technology Assets	Encrypted?	List Encryption Software	Where are private keys stored?
Database Systems	Yes ☐ No ☐		
Business Applications (if hosts PII)	Yes ☐ No ☐		
Servers	Yes ☐ No ☐		
Desktops	Yes ☐ No ☐		
Laptops	Yes ☐ No ☐		
Mobile Devices	Yes ☐ No ☐		
Backups	Yes ☐ No ☐		
Other: (specify)_____	Yes ☐ No ☐		

(d) Complete the following table with respect to PII that is transmitted from, or received by, the Applicant's Network:

Type of PII	External Source	Transmit/Receive	Encrypted?	Encryption Method
		Transmit/Receive	Yes ☐ No ☐	
		Transmit/Receive	Yes ☐ No ☐	
		Transmit/Receive	Yes ☐ No ☐	
		Transmit/Receive	Yes ☐ No ☐	
		Transmit/Receive	Yes ☐ No ☐	
		Transmit/Receive	Yes ☐ No ☐	
Example :				
Social Security Numbers	*Prescription Drug Benefit Company*	*Transmit*	*Yes*	*Site-to-Site VPN with 3DES encryption. File is then encrypted by PGP and decrypted at destination.*

(e) List the Applicant's three largest PII transfers and how often they occur.
1.
2.
3.

(f) Do you sell, share or distribute personally identifiable information to 3rd parties? Yes ☐ No ☐

If "Yes," please provide details:

If "Yes," do you always have your customers' approval before selling, sharing or distributing such information? Please explain.

4. NETWORK SECURITY

(a) Are firewalls in use within the Applicant organization? Yes ☐ No ☐

If "Yes," please outline the brand, model number, and which portion of the Network each firewall is protecting.

(b) Are Intrusion Detection Sensors or Intrusion Prevention Sensors (IDS/IPS) in place throughout the Applicant's Network? Yes ☐ No ☐

If "Yes," answer the following:
Identify the sensor brand and model:
Explain where the IDS/IPS are located:

(c) Is an Event Response Plan in place for dealing with IDS/IPS events? Yes ☐ No ☐

(d) How frequently are the firewall and Intrusion Detection System rules sets updated?

(e) Excluding firewalls and IDS/IPS, detail all other technical security devices currently protecting the Applicant organization's Network (e.g. content firewalls, other monitoring devices, etc.):

(f) Does the Applicant have consistent security standards for network endpoints? Yes ☐ No ☐

(g) Are Wireless Access Points (WAPs) available within the Applicant's environment? Yes ☐ No ☐

If "Yes," explain the role that WAPs serve within the Applicant organization:

Describe any security mechanisms currently in place for WAPs (e.g., WEP, WPA):

(h) Does the Applicant have a hard-drive, electronic and paper records destruction policy in place? Yes ☐ No ☐

If "Yes," please explain process for each:

(i) Are data leakage controls or applications installed to prevent accidental dissemination of confidential information (such as email or FTP scanning)? Yes ☐ No ☐

If "Yes," identify controls or applications in place:

(j) Has the Applicant organization conducted penetration testing? Yes ☐ No ☐

If "Yes," identify below the focus of the penetration testing:
Network based: ☐ Application based: ☐
Social based: ☐ Other (specify): ☐

Provide the names of the companies/vendors performing the last three penetration tests for the Applicant and the associated dates of the tests: ☐

(k) Does Your Data Center hold any active certifications (e.g. SAS 70, ISO 17799 adherence)? Yes ☐ No ☐

If "Yes," please list: ☐

(l) Does the Applicant organization employ regular vulnerability scanning? Yes ☐ No ☐

If "Yes," when was the last scan performed? ☐
What product was used to perform the scan? ☐
If a vendor performed the scan, what vendor? ☐

Have all critical deficiencies been addressed by Applicant? Yes ☐ No ☐

If "No," list deficiencies not addressed: ☐

5. ANTI-X DEFENSE (ANTI-VIRUS, ANTI-SPAM, ANTI-SPYWARE)

(a) Detail the Applicant's anti-virus, anti-spam and anti-spyware applications, any vendors used, and the update frequency for each component: ☐

(b) Has the Applicant organization experienced any virus infections or spyware/malware infections in the past two years? Yes ☐ No ☐

If "Yes," please provide the following information:
1. What length of time was required for remediation? ☐
2. How many workstations/servers were compromised by the infection? ☐
3. How have defenses been bolstered since the last infection? ☐

6. SOFTWARE DEVELOPMENT PATCH MANAGEMENT PHILOSOPHY

(a) Does the Applicant organization have a dedicated IT Quality Assurance or Change Management group with responsibilities for testing all new software changes? Yes ☐ No ☐

(b) Are all IT upgrades and changes tested on non-production systems before being deployed? Yes ☐ No ☐

(c) Describe the Applicant's Patch Management process for both desktop and server computing environments as well as the process for patching perimeter devices: ☐

(d) Describe how frequently patches are deployed throughout the organization and what tools are used: ☐

(e) Are all purchased and home-grown applications subject to security review? Yes ☐ No ☐

(f) Are all major software releases screened for security defects? Yes ☐ No ☐

7. INTERNET SERVICES

(a) Please list all externally facing services (public web sites, portals, e-commerce initiatives, FTP servers). If none, state "none."

(b) Does the Applicant employ a multi-tiered DMZ style extranet network for all externally facing services? Yes ☐ No ☐

(c) Is any PII stored on any of these externally facing services? Yes ☐ No ☐

If "Yes," provide details:

8. REMOTE ACCESS

(a) Is anyone permitted to connect to the Applicant's Network remotely? Yes ☐ No ☐

If "Yes," what remote computing and security mechanisms are in use?

9. BUSINESS CONTINUITY PLAN (Complete Only if Applying For Business Interruption Coverage)

(a) Please describe how the Applicant is able to conduct business in the event of a network interruption? If the Applicant's business would be totally incapacitated by a network attack, please affirm.

Please complete in full detail.

If the Applicant's network is interrupted, what is the maximum amount of revenue that would be affected if such network were to be down?

1. Six Hours
2. Twelve Hours
3. Twenty-four Hours
4. One Week

(b) Does the Applicant have a Disaster Recovery Plan in place? Yes ☐ No ☐

(c) At a high-level, please detail your Disaster Recovery Plan (recovery location/back-up site, recovery provider if applicable, external vendor dependencies, etc.):
Please complete in full detail.

(d) How long/severe does an interruption have to be for it to trigger your Disaster Recovery Plan?
Please complete in full detail.

(e) Once the Disaster Recovery Plan is triggered, how quickly do you expect your network to be back up-and-running?
Please complete in full detail.

(f) Does the Disaster Recovery Plan contemplate outages due to malicious technical events? Yes ☐ No ☐

(g) How frequently is your Disaster Recovery Plan audited and tested?

(h) If a hot-site is in use, how does the Applicant prevent potentially corrupt or malicious data from replicating to its backup site? ☐

10. PAYMENT CARD TRANSACTIONS

(a) Does the Applicant currently accept payment by credit, debit or ATM cards? Yes ☐ No ☐

If "No," please skip to Section 11.

If "Yes", complete the following:

1. Are you PCI compliant? Yes ☐ No ☐

   If "Yes", what level? ☐

   I. Please provide the name of the party which performed the last PCI audit, and the date it was completed: ☐

   II. Do you outsource your credit card processing? Yes ☐ No ☐

   If "Yes," is the processor PCI compliant? Yes ☐ No ☐

   If "Yes," is there indemnity language within the agreement with the processor eliminating your liability? Yes ☐ No ☐

   If "No," please explain: ☐

2. Estimate the amount of PII (number of records) that annually moves through the Applicant's Network as a result of these payment transactions: ☐

3. Describe the Applicant's network transmission process for such payment transactions: ☐

4. Describe in full detail the Applicant's process for credit card transactions: ☐
   Please include responses to the following:

   I. Does PII reside on the Applicant's Point Of Sale systems at any time during a credit card transaction? Yes ☐ No ☐

   If "Yes," how long does PII reside on such systems? ☐

   II. Where does the Applicant send and store PII? ☐
   III. What security measures are in place to protect PII? ☐
   IV. If PII is sent in batches, what is the size of the average batch? ☐
   How many batches are processed each day? ☐
   V. If Applicant has retail locations, how are such locations electronically connected to Applicant's corporate headquarters: ☐

5. What is the percentage of revenue breakdown between POS and e-commerce transactions? ☐

11. DATA BACK UP

(a) Do you back-up your data? Yes ☐ No ☐

If "Yes," complete the following table detailing data backups:

Type of Library	In use?	Is data encrypted?	Encryption Software In-Use
Tape Media	Yes ☐ No ☐	Yes ☐ No ☐	
Virtual Tape Library	Yes ☐ No ☐	Yes ☐ No ☐	
Hot-site Data Replication	Yes ☐ No ☐	Yes ☐ No ☐	
Electronic Vaulting	Yes ☐ No ☐	Yes ☐ No ☐	

(b) If tape media is in use, please describe the storage and transport of backup tapes: ☐

12. COMPLIANCE AND INCIDENT RESPONSE

(a) Does the Applicant organization have a documented Incident Response Plan for dealing with data breaches? Yes ☐ No ☐

If "Yes," please detail: ☐ If "No," please explain: ☐

(b) Has a dedicated information security team been established? Yes ☐ No ☐

(c) Please detail the organizational structure of the Applicant organization or attach the organizational chart. ☐

(d) Please provide the name and title of the individual responsible for establishing and maintaining information security policies within the Applicant organization: ☐

(e) HIPAA (If the Applicant does not collect Protected Health Information, please skip this question)

If the Applicant receives, stores, processes or transmits Personal Health Information (PHI), is the organization HIPAA compliant? Yes ☐ No ☐

If "Yes," please provide the name of the party which performed the last HIPAA audit, and the date it was completed: ☐

(f) Does the Applicant conduct business in the European Union (EU)? Yes ☐ No ☐

If "Yes," is the Applicant subject to EU information privacy and consumer protection laws?

Yes ☐ No ☐

(g) How does the Applicant maintain compliance with those laws? ☐

(h) Are you subject to any international notification statutes? Yes ☐ No ☐

If "Yes," identify such statutes. ☐

(i) In how many U.S. states does the Applicant have customers (including on-line customers)? (If unable to provide an exact number, please provide a best estimate, and indicate that the number provided is an estimate.) ☐

13. THIRD PARTY ACCESS CONTROLS

(a) Does the Applicant provide independent contractors, vendors, or other individuals or entities outside the Applicant organization ("third parties") to have access either to its Network, or to PII including PHI, which is received, stored, processed or transmitted on the Applicant's Network?

Yes ☐ No ☐

If "Yes," describe how the organization monitors and restricts access by third parties to sensitive parts of the Network, or access to PII including PHI:

If "Yes," are the access attempts by these third parties logged? Yes ☐ No ☐

(b) When third parties have access to PHI, are they required to sign a Business Associate Agreement? Yes ☐ No ☐

If "Yes," do they also sign a Security Addendum? Yes ☐ No ☐

Please attach a copy of a sample Business Associate Agreement and Security Addendum, if used.

(c) Does the Applicant always require third parties to carry their own errors and omissions insurance? Yes ☐ No ☐

If "Yes," at what Limit of Liability?
If "No," explain:

14. USER CONTROLS

(a) For employees or third parties that have access to PII, please indicate if the Applicant performs the following prior to retaining such individual:

background checks Yes ☐ No ☐
drug testing Yes ☐ No ☐
credit checks Yes ☐ No ☐
reference checks Yes ☐ No ☐

If "No," describe the checks that are performed:

(b) What is the control process for granting employees or third parties access to PII, including PHI?

(c) System Password Controls:

1. Are passwords set to expire on an interval basis? Yes ☐ No ☐

   If "Yes," at what intervals?

2. Describe what complexity controls are in place to enforce strong passwords?

3. Are these password controls in place across all major applications? Yes ☐ No ☐

15. MEDIA & INTELLECTUAL PROPERTY

(a) Does any of the matter disseminated by Your Company contain the following types of content (please check those which apply)?

Alternative	☐	Expose/Investigate	☐	Medical Diagnostics	☐
Social Commentary	☐	Celebrity	☐	How-To/ Technical	☐
Music	☐	Unauthorized Biography	☐	Controversial	☐
Mature/Adult	☐	Religious	☐	None of the Above	☐

If none of the above, please describe the types of content which is included in an matter disseminated by the Applicant organization: ☐

(b) Does the Applicant have a formal and active review process to screen matter, including online content and content provided by third parties, for the following offenses prior to dissemination, publication, broadcast, or distribution (check all that apply)?

Privacy Violations	Yes ☐ No ☐
Defamation	Yes ☐ No ☐
Trademark Infringement	Yes ☐ No ☐
Copyright Infringement	Yes ☐ No ☐
Other ☐	

(c) Check the Intellectual Property ("IP") protections employed in the Applicant's business:

IP Controls	Stage of Use		
	Not Started	In Progress	Complete and Regularly in use
IP protection within Employee Agreements			
IP protection within Non-Disclosure Agreements (NDA) with all 3rd parties			
Prior Art Searches by legal professional (internal or external)			
Acquisition of all necessary IP rights via licenses, releases, or consents			
Annual training of employees regarding patent, copyright, and trademark issues			
Acquire written permission of internet sites You link to or frame			

16. ACTUAL OR POTENTIAL CLAIMS

(a) During the last five years, have any Claims, suits or regulatory proceedings been brought against any party proposed for coverage? Yes ☐ No ☐

(b) During the last five years, has any party proposed for coverage given notice to any previous insurance carrier of any fact, situation or circumstance which is expected to result in a Claim, suit or regulatory proceeding against any party proposed for coverage? Yes ☐ No ☐

(c) Is any party proposed for coverage, currently aware of any fact, situation or circumstance which could give rise to a Claim, suit or regulatory proceeding against any party proposed for coverage? Yes ☐ No ☐

WITHOUT PREJUDICE TO ANY OTHER RIGHTS AND REMEDIES OF THE INSURER, IT IS AGREED THAT ANY MATTER REQUIRED TO BE DISCLOSED IN RESPONSE TO THE ABOVE QUESTIONS IN THIS SECTION 16, AND ANY CLAIM, SUIT OR PROCEEDING ARISING FROM OR RELATED TO SUCH MATTER, IS EXCLUDED FROM ALL PROPOSED INSURANCE.

17. ADDITIONAL APPLICATION MATERIALS

Please attach a copy of the following materials:

- Any specific Claim or Potential Claim information including but not limited to the claimant's name, allegations made, status of claim, suit, or proceeding, the amount of incurred defense expenses and total amount paid in judgment or settlement.
- The most recent fiscal year-end and interim financial statements.
- The most recent edition of the Applicant's Privacy Policy.
- A sample copy of Applicant's Business Associate Agreement and associated Security Addendum.

18. NOTICES TO APPLICANT

The Undersigned warrants that, to the best of his or her knowledge and belief, the statements set forth herein are true and accurate. The Insurer will have relied upon this Application in issuing any policy. The Insurer is hereby authorized to make any investigations and inquiry in connection with the information, statements and disclosures provided in this Application.

The signing of the Application does not bind the Undersigned to purchase the insurance, nor does review of this Application bind the Insurer to issue a policy. It is agreed that this Application shall be the basis of the contract should a policy be issued. This Application shall be attached and will become part of the policy. 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.

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

- **The Policy shall apply only to Claims made during the Policy Period or Extended Reporting Period (if applicable);**
- **The Limit of Liability referenced in the Policy shall be reduced by, and may be completely exhausted by, the payment of Defense Expenses. In such event, the Insurer shall not be liable for the payment of Defense Expenses, or bear the responsibility of defending or continuing to defend any Claim, or be liable for the amount of any judgment or settlement, to the extent that such costs exceed the Limit of Liability referenced in the Policy; and**
- **Defense Expenses that are incurred shall be applied against the Retention amount.**

19. MATERIAL CHANGE

The Undersigned declares that if any occurrence or event takes place prior to the effective date of the insurance for which this Application is being made, which may render inaccurate, untrue, or incomplete any statement made in this Application or any attachment thereto, such occurrence or event will immediately be reported in writing to the Insurer. The Insurer may withdraw or modify any outstanding quotations and/or authorization or agreement to bind the insurance.

20. FRAUD WARNINGS

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. NOTHING CONTAINED HEREIN OR INCORPORATED HEREIN BY REFERENCE SHALL CONSTITUTE NOTICE OF A CLAIM OR POTENTIAL CLAIM SO AS TO TRIGGER COVERAGE UNDER ANY CONTRACT OF INSURANCE.

NOTICE TO ARKANSAS 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 FINES AND CONFINEMENT IN PRISON."

NOTICE TO 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 POLICYHOLDER OR CLAIMANT FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE POLICYHOLDER 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."

NOTICE TO DISTRICT OF COLUMBIA APPLICANTS: "WARNING: IT IS A CRIME TO PROVIDE FALSE OR MISLEADING INFORMATION TO AN INSURER FOR THE PURPOSE OF DEFRAUDING THE INSURER OR ANY OTHER PERSON. PENALTIES INCLUDE IMPRISONMENT AND/OR FINES. IN ADDITION, AN INSURER MAY DENY INSURANCE BENEFITS IF FALSE INFORMATION MATERIALLY RELATED TO A CLAIM WAS PROVIDED BY THE APPLICANT."

NOTICE TO 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."

NOTICE TO HAWAII APPLICANTS: "FOR YOUR PROTECTION, HAWAII LAW REQUIRES YOU TO BE INFORMED THAT PRESENTING A FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT IS A CRIME PUNICHABLE BY FINES OR IMPRISONMENT, OR BOTH."

NOTICE TO KENTUCKY APPLICANTS: "ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE 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."

NOTICE TO LOUISIANA 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 FINES AND CONFINEMENT IN PRISON."

NOTICE TO MAINE 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."

NOTICE TO NEW JERSEY APPLICANTS: "ANY PERSON WHO INCLUDES ANY FALSE OR MISLEADING INFORMATION ON AN APPLICATION FOR AN INSURANCE POLICY IS SUBJECT TO CRIMINAL AND CIVIL PENALTIES."

NOTICE TO 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."

NOTICE TO 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, 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."

NOTICE TO OHIO APPLICANTS: "ANY PERSON WHO, WITH INTENT TO DEFRAUD OR KNOWING THAT HE IS FACILITATING A FRAUD AGAINST AN INSURER, SUBMITS AN APPLICATION OR FILES A CLAIM CONTAINING A FALSE OR DECEPTIVE STATEMENT IS GUILTY OF INSURANCE FRAUD."

NOTICE TO 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" (365:15-1-10, 36 §3613.1).

NOTICE TO 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."

NOTICE TO TENNESSEE 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."

NOTICE TO TEXAS APPLICANTS: "ANY PERSON WHO KNOWLINGLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR THE PAYMENT OF A LOSS IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN STATE PRISON."

NOTICE TO VERMONT APPLICANTS: "ANY PERSON WHO KNOWINGLY PRESENTS A FALSE STATEMENT IN AN APPLICATION FOR INSURANCE MAY BE GUILTY OF A CRIMINAL OFFENSE AND SUBJECT TO PENALTIES UNDER STATE LAW."

NOTICE TO VIRGINIA 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 INCLUDE IMPRISONMENT, FINES AND DENIAL OF INSURANCE BENEFITS."

NOTICE TO 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."

NOTICE TO WEST VIRGINIA APPLICANTS: "ANY PERSON WHO KNOWINGLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR THE PAYMENT OF A LOSS OR THE BENEFIT OR KNOWINGLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON."

NOTICE TO ALL OTHER 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."

NAME (PLEASE PRINT): _____ TITLE:_____

SIGNATURE: _____ DATE:_____