



**APPLICATION FOR ARCH NETSAFE® 2.0**  
**NETWORK SECURITY & PRIVACY, TECHNOLOGY, E&O & MEDIA INSURANCE**

**NOTICE: THE LIABILITY COVERAGE PARTS OF THIS POLICY PROVIDE CLAIMS MADE COVERAGE. EXCEPT AS OTHERWISE PROVIDED, SUCH COVERAGE APPLIES ONLY TO CLAIMS FIRST MADE AGAINST THE INSUREDS DURING THE POLICY PERIOD AND REPORTED TO THE INSURER NO LATER THAN 60 DAYS AFTER THE END OF THE POLICY PERIOD. EACH APPLICABLE LIMIT OF LIABILITY SHALL BE REDUCED, AND MAY BE EXHAUSTED, BY DEFENSE COSTS PAYMENTS. IF ANY LIMIT OF LIABILITY IS EXHAUSTED, THE INSURER SHALL HAVE NO FURTHER LIABILITY FOR THE COVERAGE TO WHICH SUCH LIMIT APPLIES, INCLUDING LIABILITY FOR DEFENSE COSTS. ALL LOSS PAYMENTS, INCLUDING DEFENSE COSTS PAYMENTS, SHALL APPLY TO THE RETENTION.**

**NOTICE: A POLICY WILL NOT BE ISSUED UNLESS THE APPLICATION IS PROPERLY COMPLETED, SIGNED AND DATED.**

**NOTICE: THIS APPLICATION, INCLUDING ANY INFORMATION AND MATERIALS SUBMITTED WITH THIS APPLICATION, SHALL BE HELD IN CONFIDENCE.**

**Instructions for Completing This Application**

Please read carefully, fully answer all questions, and submit all requested information for each coverage applied for. Attach additional pages if more space is required to answer a question or respond to information request. As used herein, "Applicant" means the organization specified in item 1 below and each entity controlled by such organization for which coverage is applied for. Checking any box labeled "N/A" means that the information requested is not applicable to the operations of the Applicant.

**NAME, ADDRESS, AND CONTACT INFORMATION**

Name of Applicant:

Principal Address:

City:

State:

Zip Code:

Date of Formation:

Website Address:

Name of Contact Person:

Contact Person E-Mail Address:

**GENERAL INFORMATION**

Description of Business Operations:

Names and Locations of Subsidiaries or  
Affiliates for which coverage is desired:

Number of Branch Offices:

Number of Employees:

Number of Server Locations:

## FINANCIAL INFORMATION

Gross Revenue Past 12 Months	Projected Revenue Next 12 Months	% of Revenues Outside the US:
\$ _____	\$ _____	_____ %

Are you presently involved in or considering any merger, acquisition or change in control? ☐ No ☐ Yes  
If yes, please explain \_\_\_\_\_

### COVERAGE REQUESTED

Please check each coverage applied for and insert the requested limit of liability

Coverage Part		Limit of Liability
A. Network Security & Privacy Liability	<input type="checkbox"/>	\$ _____
B. Media Liability	<input type="checkbox"/>	\$ _____
C. Technology Services and Products and Professional Liability	<input type="checkbox"/>	\$ _____
D. Data Incident Response Expense	<input type="checkbox"/>	\$ _____
E. Business Interruption	<input type="checkbox"/>	\$ _____
F. Cyber Extortion	<input type="checkbox"/>	\$ _____

### COMPLIANCE AND DATA INFORMATION (Complete if Coverage A, D or F is Requested)

- Please identify the private information being stored or processed, including that of your own employees (check all that apply and provide the approximate number of records):
  - Number of records transmitted or processed per year
  - Maximum number of records stored at any one time

Social security number or taxpayer ID number	a. _____ b. _____
Drivers license number, passport number, or any other state or federal identification number	a. _____ b. _____
Medical or healthcare data including protected health information	a. _____ b. _____
Financial account record	a. _____ b. _____
Proprietary business information	a. _____ b. _____
3 <sup>rd</sup> Party confidential information	a. _____ b. _____

- For the private information collected, is there a process for deleting this information once it is complete or not needed anymore? Yes ☐ No ☐

3. Are you compliant with the following (if no, please explain on a separate attachment):
  - a. Health Insurance Portability and Accountability Act (HIPAA) Yes ☐ No ☐ N/A ☐
  - b. Gramm-Leach Bliley Act of 1999 (GLBA) Yes ☐ No ☐ N/A ☐
4. For HIPAA, GLBA and/or other state or federal regulation compliance, what due diligence/auditing is performed to ensure that you remain in compliance and what individual(s) in your organization are responsible for said compliance? \_\_\_\_\_
5. In the next 12 months will you accept, store, process, or exchange credit/debit card transaction information? Yes ☐ No ☐
  - a. If yes, what is your PCI/DSS certification level: I ☐ II ☐ III ☐ IV ☐
  - b. Have you had a PCI compliance audit performed in the last 12 months by an approved PCI Qualified Security Assessor? Yes ☐ No ☐ If no, please explain: \_\_\_\_\_
6. Approximately how many credit/debit card transactions do you expect to handle in the next 12 months companywide: \_\_\_\_\_
7. Approximately how many credit/debit card account numbers do you have stored companywide? \_\_\_\_\_

#### NETWORK SECURITY & EMPLOYEE CONTROLS (Complete if Coverage A, D or F is Requested)

If you answer NO to any of the questions below please explain in a separate attachment.

1. Check all that apply and name the service provider for each category (please attach a copy of the representative contract/agreement):

Type		Supplier Name or N/A
a. Hosting Facility	<input type="checkbox"/>	_____
b. Co-location Facility	<input type="checkbox"/>	_____
c. Managed Security Service Provider (MSSP)	<input type="checkbox"/>	_____
d. Application Service Provider (ASP)	<input type="checkbox"/>	_____
e. Data Storage Facility	<input type="checkbox"/>	_____
f. Payroll	<input type="checkbox"/>	_____
g. Benefits	<input type="checkbox"/>	_____
h. Other Human resource functions	<input type="checkbox"/>	_____
i. Other (please specify)	<input type="checkbox"/>	_____

2. Do you have any data sharing agreements with any 3<sup>rd</sup> parties? Yes ☐ No ☐ (Please attach a copy of the contracts/agreements)
  - a. Do you have contracts in place with the 3<sup>rd</sup> parties that require the vendor to maintain controls, practices and procedures that are as protective as your own internal procedures? Yes ☐ No ☐

Do the contracts require the 3<sup>rd</sup> parties to defend and indemnify you for liability arising from their use of the data they are handling? Yes ☐ No ☐

3. Do you regularly audit 3<sup>rd</sup> parties with whom you have data sharing agreements with? Yes ☐ No ☐  
a. If no, how do you ensure their compliance with HIPAA, PCI, etc.? \_\_\_\_\_
4. Does your company have a current information security policy that has been approved by executive management? Yes ☐ No ☐  
a. If yes, does the policy specify acceptable use of all company resources including the proper use of email and the Internet? Yes ☐ No ☐  
b. If yes, are all employees provided with a copy of the policy? Yes ☐ No ☐  
c. If yes, are all employees required to provide written confirmation they have read and understood the contents of the policy? Yes ☐ No ☐
5. Is there an information classification program that specifies different levels of security based on the nature of a given information asset? Yes ☐ No ☐  
a. If yes, are user accounts audited regularly to determine their security levels are appropriately set? Yes ☐ No ☐
6. Does your company have an information security officer? Yes ☐ No ☐
7. Are documented procedures in place for user and password management and are they monitored for compliance? Yes ☐ No ☐ Do you have a process for managing user accounts including promptly deleting or modifying access upon a change of responsibilities or termination? Yes ☐ No ☐
8. Are special privileges restricted to systems administration personnel with an approved need to have these privileges? Yes ☐ No ☐  
Provide a brief description of the measures taken to ensure the physical security of computer systems from unauthorized entry/access. \_\_\_\_\_
9. Is there a patch management process in place? Yes ☐ No ☐ if yes, what is the timeframe for implementing patches following identification? \_\_\_\_\_
10. Is firewall technology used to prevent unauthorized access to and from internal networks and external networks? Yes ☐ No ☐ Are firewall configurations regularly reviewed and kept up to date? Yes ☐ No ☐
11. Is anti-virus software installed on all computers/servers that connect to your network? Yes ☐ No ☐  
a. Is the anti-virus software package updated regularly? Yes ☐ No ☐ How often? \_\_\_\_\_  
b. Are the virus signature files updated daily (or in close step with updates provided by the software company)? Yes ☐ No ☐  
c. Is there an appropriately trained security analyst on staff to assist in identifying and mitigating incidents involving undetected malware? Yes ☐ No ☐  
d. Are systems regularly audited to identify inappropriate code and/or applications that have been installed? Yes ☐ No ☐
12. Do you allow remote access to your system? Yes ☐ No ☐ If yes, what controls are in place to prevent unauthorized access? \_\_\_\_\_
13. Do you or any third parties conduct any penetration & vulnerability testing? Yes ☐ No ☐ If yes, have any major findings been remediated? \_\_\_\_\_ If no, please explain.



14. Do you monitor security alerts and advisories from your system vendors, Computer Emergency Response Team (CERT) and other sources, taking appropriate and responsive actions? Yes ☐ No ☐
15. Do you monitor your network in real time to detect possible intrusions or abnormalities in the performance of your system? Yes ☐ No ☐ If no, please explain how you monitor your network. \_\_\_\_\_
16. Do you monitor log files on a regular basis to help spot abnormal trends? Yes ☐ No ☐ For how long are log files maintained? \_\_\_\_\_
17. Is your security policy reviewed and updated at least annually? Yes ☐ No ☐
18. Does your hiring process include the following (check all that are applicable):
- |                           | All Employees            | Some Employees           | Ind. Cont.               | Not Required             |
|---------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Criminal Background Check | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Drug Tests                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Work History Verification | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Educational Verification  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Credit Check              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

If checks are only required in some circumstances but not others, please explain.

19. In the past 12 months, have you had layoffs or do you anticipate layoffs in the coming 12 months?  
Yes ☐ No ☐ If yes, please explain:

**PRIVACY CONTROLS** (Complete if Coverage A, D or F is Requested)

1. Do you have a privacy policy? Yes ☐ No ☐
2. Is your privacy policy posted on your website and made available to your customers prior to them providing personal information? Yes ☐ No ☐
3. Is your privacy policy reviewed and updated at least annually? Yes ☐ No ☐
4. Do you sell or share the personal subscriber/customer information with other unaffiliated 3<sup>rd</sup> parties? Yes ☐ No ☐
  - a. If yes, do you provide opt-out controls that are visible and addressed within the privacy policy? Yes ☐ No ☐
  - b. Do you notify customers upon the release of their private information? Yes ☐ No ☐
5. Do you train employees on the proper handling of private information? Yes ☐ No ☐
6. Do you utilize retained private information in any other way than originally intended or disclosed? Yes ☐ No ☐ If yes, please explain: \_\_\_\_\_
7. Do you have a document retention and destruction policy? Yes ☐ No ☐ Please explain: \_\_\_\_\_
8. Do you have policies/procedures in place for handling employees that are terminated or leave voluntarily? Yes ☐ No ☐
  - a. Does the policy specifically address their access to corporate applications and personal information including proprietary corporate information? Yes ☐ No ☐
9. Do you conduct an annual privacy assessment to ensure that you are in compliance with privacy laws and regulations? Yes ☐ No ☐ If no, Please explain: \_\_\_\_\_
10. Are procedures in place to escalate any incidents of a breach or possible breach of private information? Yes ☐ No ☐
11. Do you ensure that all private information is encrypted whether at rest or in transit? Yes ☐ No ☐
  - a. If not technically feasible, what safeguards are in place to ensure the security of private information? \_\_\_\_\_
  - b. If Data and/or Private Information is not in electronic form, what precautions are taken to ensure its security? \_\_\_\_\_
12. Is data (i.e. personal information) encrypted on laptops and other mobile devices used for storing and transferring data? Yes ☐ No ☐
13. Do you allow sensitive data to be loaded on to devices that may be removed from the premises? Yes ☐ No ☐

**MEDIA CONTROLS** (Complete if Coverage B is Requested)

1. Do you publish a bulletin board, chat room or otherwise allow users to upload or post content to your website? Yes ☐ No ☐  
If yes, do you have a process for monitoring, approving and removing such content? Yes ☐ No ☐

2. Do you have legal review of your content performed by staff or outside attorney? Yes ☐ No ☐ If no, what review is being completed? \_\_\_\_\_
3. Is legal review performed on all intellectual property utilized in the course of your business operations? Yes ☐ No ☐ N/A ☐
4. Do you have written clearance procedures in place regarding use, licensing, and consent agreements for third party content used by you in your products or services and on your website or in your promotional materials? Yes ☐ No ☐ If no, please explain: \_\_\_\_\_
5. Do you have written guidelines for your use of social media and its use by your employees? Yes ☐ No ☐ If no, please explain: \_\_\_\_\_

**ERRORS & OMISSIONS/TECHNOLOGY CONTROLS (Complete if Coverage C is Requested)**

1. Describe professional services and/or technology products/services for which coverage is desired and provide the associated revenues for each service (attach a separate sheet if necessary):

PROFESSIONAL SERVICE/TECHNOLOGY PRODUCT/SERVICE	REVENUES PAST 12 MONTHS

2. List the firm's largest clients:

CLIENT	PROFESSIONAL SERVICE/TECHNOLOGY PRODUCT/SERVICE	REVENUES PAST 12 MONTHS

3. Please describe the types of negligent acts, errors, omissions incidents, circumstances or exposures that you believe could result in a professional liability or errors and omissions claim:
4. Describe any procedures, precautions or safeguards you use to avoid such claims (e.g. Quality control procedures, testing procedures etc.):
5. Do you have a formal procedure in place for handling customer complaints? Yes ☐ No ☐

6. Do you require customer sign-off on mid-project changes? Yes ☐ No ☐

7. Do you have written contracts or agreements with each client? Yes ☐ No ☐

If no:

- a. \_\_\_\_\_ What percent of time are contracts not used? \_\_\_\_\_ %
- b. What governs the performance of services in the absence of a contract? \_\_\_\_\_

8. Do your standard contracts or service agreements contain the following provisions?

- a. Arbitration Clause? Yes ☐ No ☐
- b. Limitation of Liabilities to your benefit? Yes ☐ No ☐
- c. Exclusive Remedy? Yes ☐ No ☐
- d. Exclusion of consequential damages? Yes ☐ No ☐
- e. Indemnification Clause to your benefit? Yes ☐ No ☐

9. What percentage of contracts deviate from your standard provisions listed in 7. above? \_\_\_\_\_ %

10. Who has authority to customize contracts? \_\_\_\_\_

11. Who has authority to commit the applicant to contracts? \_\_\_\_\_

12. What is the range of the limitation of liability in contracts? \_\_\_\_\_

13. What is the average contract value and duration? \$ \_\_\_\_\_ Months

14. What percentage of revenues is generated from services provided by sub-contractors? \_\_\_\_\_ %

15. Do you require sub-contractors to carry E&O insurance? Yes ☐ No ☐

16. If you provide a technology service, do you test products for malicious code or other security flaws? Yes ☐ No ☐

#### **BUSINESS INTERRUPTION CONTROLS (Complete if Coverage E is Requested)**

1. Percent of revenues that are network dependent: \_\_\_\_\_ %

2. Are system backup and recovery procedures documented and regularly tested for all mission critical systems/websites? Yes ☐ No ☐ If no, how often? \_\_\_\_\_

3. Are network and system backups performed at least once per week? Yes ☐ No ☐

4. Are there redundant connections to you critical business partners? Yes ☐ No ☐

5. Do you have a written business continuity/disaster recovery plan that includes procedures to be followed in the event of a disruptive computer incident? Yes ☐ No ☐

6. What is your estimated recovery time for critical systems to restore operations after a cyber attack or other loss/corruption?

#### **PRIOR LOSSES, CIRCUMSTANCES, & EVENTS (Required for All Applicants)**

**IF YOU ANSWER YES TO ANY OF THESE QUESTIONS PLEASE ATTACH SEPARATE SHEET(S) WITH A FULL DESCRIPTION OF EACH INCLUDING DATES, ALLEGATIONS, CIRCUMSTANCES, COSTS, SETTLEMENT/JUDGEMENT AMOUNTS, ETC.**

1. During the last 3 years, have you had any information security breaches including unauthorized access, unauthorized use, denial of service attack, breach, theft of data, fraud, electronic vandalism, sabotage or other security events. Yes ☐ No ☐
2. During the last 3 years, has anyone alleged that you were responsible for damages to their systems arising out of the operation of your system? Yes ☐ No ☐
3. During the last 3 years, have you received a complaint or an injunction arising out of intellectual property infringement, content or advertising? Yes ☐ No ☐
4. During the last 3 years, has anyone made a demand, claim, complaint, or filed a lawsuit against you that would or could be covered under this policy? Yes ☐ No ☐
5. During the last 3 years, have you been the subject of an investigation or action by any regulatory or administrative agency for privacy related violations? Yes ☐ No ☐
6. Has any application for similar insurance been declined or has any such insurance ever been rescinded, cancelled or been refused renewal? Yes ☐ No ☐
7. During the last 3 years, have you experienced a disruption to your computer system that lasted longer than 4 hours for any reason (other than planned downtime)? Yes ☐ No ☐

**PRIOR KNOWLEDGE – ALL COVERAGE PARTS (DO NOT COMPLETE FOR RENEWAL APPLICATIONS)**

8. Are you aware of any circumstance or event that could result in a claim being made against the policy being applied for? Yes ☐ No ☐

**IT IS AGREED THAT ANY LOSS ARISING FROM, BASED UPON, OR ATTRIBUTABLE TO ANY EVENT OR CIRCUMSTANCE OF WHICH ANY PERSON OR ENTITY HAS ANY KNOWLEDGE OR INFORMATION WILL BE EXCLUDED FROM COVERAGE UNDER THE PROPOSED INSURANCE**

**ADDITIONAL INFORMATION REQUIRED:**

Privacy Policy

Most Current Audited Financial Statements.

If Coverage C. Technology Services and Products and Professional Liability coverage is desired, also include:

- a) a standard contract representative of the services provided including promotional material, and
- b) Resumes of key professionals

**APPLICATION MUST BE SIGNED AND DATED BY AN AUTHORIZED OFFICER, PARTNER OR PRINCIPAL.**

**THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE COMPANY, NOR DOES IT OBLIGATE THE COMPANY TO ISSUE A POLICY OR INSURE ANY SERVICES. HOWEVER, IT IS AGREED THAT SHOULD A POLICY BE ISSUED, THIS APPLICATION WILL BE ATTACHED TO AND MADE A PART OF THE POLICY.**

**THE UNDERSIGNED(S) CERTIFIES THAT HE/SHE IS THE DULY AUTHORIZED REPRESENTATIVE(S) OF EACH PROPOSED INSURED WHICH SUBMITS THIS APPLICATION FOR A POLICY OF INSURANCE. THE STATEMENTS AND INFORMATION ABOVE AND ALL SCHEDULES AND DOCUMENTS SUBMITTED, OF WHICH THE UNDERWRITER RECEIVES NOTICE, ARE DEEMED PARTS OF THE APPLICATION (ALL OF WHICH SCHEDULES AND DOCUMENTS SHALL BE DEEMED ATTACHED TO THE POLICY AS IF PHYSICALLY ATTACHED THERETO), AND THE WORD "APPLICATION" REFERS TO ALL OF THE FOREGOING.**

**EACH PROPOSED INSURED REPRESENTS THAT THE STATEMENTS SET FORTH IN THE APPLICATION ARE TRUE AND CORRECT, AND THAT REASONABLE EFFORTS HAVE BEEN MADE TO OBTAIN INFORMATION SUFFICIENT FOR ACCURATE COMPLETION OF THIS APPLICATION. IT IS FURTHER AGREED BY EACH PROPOSED INSURED THAT EACH POLICY OR RENEWAL THEREOF, IF ISSUED, IS ISSUED IN RELIANCE UPON THE TRUTH OF THE REPRESENTATIONS AND INFORMATION IN THE APPLICATION.**

**EACH PROPOSED INSURED UNDERSTANDS AND AGREES THAT ANY INSURANCE POLICY ISSUED BY THE COMPANY SHALL BE SUBJECT TO RESCISSION IF THIS APPLICATION CONTAINS ONE OR MORE MISREPRESENTATIONS OR OMISSIONS MATERIAL TO THE ACCEPTANCE OF THE RISK BY THE COMPANY.**

**IF THE INFORMATION SUPPLIED ON THIS APPLICATION OR ATTACHMENTS THERETO CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE INCEPTION DATE OF THE POLICY, THE APPLICANT WILL IMMEDIATELY NOTIFY THE COMPANY OF SUCH CHANGES.**

**NOTICE: ANY PERSON WHO, KNOWINGLY OR WITH INTENT TO DEFRAUD OR TO FACILITATE A FRAUD AGAINST ANY INSURANCE COMPANY OR OTHER PERSON, SUBMITS AN APPLICATION OR FILES A CLAIM FOR INSURANCE CONTAINING FALSE, DECEPTIVE OR MISLEADING INFORMATION MAY BE GUILTY OF INSURANCE FRAUD.**

**NOTICE TO ALABAMA APPLICANTS:** Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit, or who knowingly presents false information in an application for insurance is guilty of a crime and may be subject to restitution or confinement in prison, or any combination thereof.

**NOTICE TO ARKANSAS, LOUISIANA, NEW MEXICO, RHODE ISLAND AND WEST VIRGINIA 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 in the third degree.

**NOTICE TO KANSAS APPLICANTS:** 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 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 commits a fraudulent insurance act.

**NOTICE TO KENTUCKY APPLICANTS:** Any person who knowingly and with the 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 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 include imprisonment, fines and denial of insurance benefits.

**NOTICE TO MARYLAND APPLICANTS:** Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly or willfully 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 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 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 claims 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.

**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

**NOTICE TO OREGON APPLICANTS:** Any person who, knowingly and with intent to defraud or facilitate a fraud against any insurance company or other person, submits an application, or files a claim for insurance containing any false, deceptive, or misleading material information may be guilty of insurance fraud.

**NOTICE TO PENNSYLVANIA APPLICANTS:** Any person who knowingly and with the 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 PUERTO RICO APPLICANTS:** Any person who knowingly and with the intent to defraud, presents false information in an insurance request form, or who presents, helps, or has presented a fraudulent claim for the payment of a loss or other benefit, or presents more than one claim for the same damage or loss, will incur a felony, and upon conviction will be penalized for each violation with a fine of no less than five thousand dollars (\$5,000) nor more than ten thousand dollars (\$10,000); or imprisonment for a fixed term of three (3) years, or both penalties. If aggravated circumstances prevail, the fixed established imprisonment may be increased to a maximum of five (5) years; if attenuating circumstances prevail, it may be reduced to a minimum of two (2) years.

---

**SIGNED BY AUTHORIZED OFFICER, PARTNER OR PRINCIPAL**

---

**PRINT OR TYPE NAME & TITLE**

---

**PHONE NUMBER**

---

**DATE**