



## BEAZLEY BREACH RESPONSE

## APPLICATION

NOTICE: THIS POLICY'S LIABILITY INSURING AGREEMENTS PROVIDE COVERAGE ON A CLAIMS MADE AND REPORTED BASIS AND APPLY ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR THE OPTIONAL EXTENSION PERIOD (IF APPLICABLE) AND REPORTED TO THE UNDERWRITERS IN ACCORDANCE WITH THE TERMS THIS POLICY. AMOUNTS INCURRED AS CLAIMS EXPENSES UNDER THIS POLICY WILL REDUCE AND MAY EXHAUST THE LIMIT OF LIABILITY AND ARE SUBJECT TO RETENTIONS.

PLEASE READ THIS POLICY CAREFULLY.

Please fully answer all questions and submit all requested information.

### GENERAL INFORMATION:

Full Name:			
Mailing Address:		State of Incorporation:	
City:		State & Zip:	
# of Employees:		Date Established:	
Website URL's:			
Authorized Officer <sup>1</sup> :		Telephone:	
		E-mail:	
Breach Response Contact <sup>2</sup> :		Telephone:	
		E-mail:	
Business Description:			
Does the Applicant provide data processing, storage or hosting services to third parties?		<input type="checkbox"/> Yes	<input type="checkbox"/> No

### REVENUE INFORMATION:

\*For Applicants in Healthcare: Net Patient Services Revenue plus Other Operating Revenue

\*For all other Applicants, please provide Gross Revenue information

	Most Recent Twelve (12) months: (ending: ____/____)	Previous Year	Next Year (estimate)
US Revenue:	USD	USD	USD
Non-US Revenue:	USD	USD	USD
Total:	USD	USD	USD

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

<sup>1</sup> This is the officer of the Applicant that is authorized make statements to the Underwriters on the Applicant's behalf and to receive notices from the Insurer or its authorized representative(s).

<sup>2</sup> This is the employee of the Applicant that is designated to work with the insurer in response to a data breach event.

What percentage of the Applicant's revenues is business to business?      %      Direct to consumer?      %	
Are significant changes in the nature or size of the Applicant's business anticipated over the next twelve (12) months? Or have there been any such changes within the past twelve (12) months?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If 'Yes', please explain:	
Has the Applicant within the past twelve (12) months completed or agreed to, or does it contemplate entering into within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If 'Yes', please explain:	

## PRIVACY

Please identify the types of personal information of individuals that you collect, process or store (check all that apply) along with an estimate of the number of records held for each type of information:

Type of Information	Number of Records (Estimated)
<input type="checkbox"/> Social Security Numbers	<input type="checkbox"/> <100K; <input type="checkbox"/> 100K-500K; <input type="checkbox"/> 500K-1M; <input type="checkbox"/> 1M-2M; <input type="checkbox"/> 2M-5M; <input type="checkbox"/> >5M
<input type="checkbox"/> Consumer Financial Information	<input type="checkbox"/> <100K; <input type="checkbox"/> 100K-500K; <input type="checkbox"/> 500K-1M; <input type="checkbox"/> 1M-2M; <input type="checkbox"/> 2M-5M; <input type="checkbox"/> >5M
<input type="checkbox"/> Payment Card Information	<input type="checkbox"/> <100K; <input type="checkbox"/> 100K-500K; <input type="checkbox"/> 500K-1M; <input type="checkbox"/> 1M-2M; <input type="checkbox"/> 2M-5M; <input type="checkbox"/> >5M
<input type="checkbox"/> Protected Health Information	<input type="checkbox"/> <100K; <input type="checkbox"/> 100K-500K; <input type="checkbox"/> 500K-1M; <input type="checkbox"/> 1M-2M; <input type="checkbox"/> 2M-5M; <input type="checkbox"/> >5M
<input type="checkbox"/> Biometric Information	<input type="checkbox"/> <100K; <input type="checkbox"/> 100K-500K; <input type="checkbox"/> 500K-1M; <input type="checkbox"/> 1M-2M; <input type="checkbox"/> 2M-5M; <input type="checkbox"/> >5M

☐ Other (please describe):

Has the Applicant designated a Chief Privacy Officer? ☐ Yes   ☐ No

If 'No' please indicate what position(s) (if any) are responsible for privacy issues:

Does the Applicant require third parties with which it shares personally identifiable or confidential information to indemnify the Applicant for legal liability arising out of the release of such information due to the fault or negligence of the third party? ☐ Yes   ☐ No

## PAYMENT CARDS

Does the Applicant accept payment cards for goods sold or services rendered? ☐ Yes   ☐ No

If 'Yes': How many payment card transactions does the Applicant transact per year?

Is the Applicant compliant with applicable data security standards issued by financial institutions the Applicant transacts business with (e.g. PCI standards)? ☐ Yes   ☐ No

Is payment card data encrypted at the point of sale (e.g., payment card reader or e-commerce payment portal) through transmission to the payment processor? ☐ Yes   ☐ No

If the Applicant is not compliant with applicable data security standards, please describe the current status of any compliance work and the estimated date of completion:

## COMPUTER & NETWORK SECURITY

Has the Applicant designated a Chief Information Security Officer as respects computer systems and data security? ☐ Yes   ☐ No

If 'No', please indicate what position is responsible for computer and data security:		
Does the Applicant publish and distribute written policies and procedures regarding computer and information security to its employees?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Does the Applicant conduct computer and information security training for every employee that has access to computer systems or sensitive data?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Does the Applicant enforce a process for the timely installation of software updates/patches?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
If 'Yes', are critical updates/patches installed within thirty (30) days of release?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Does the Applicant restrict user rights on computer systems such that individuals (including third party service providers) have access only to those areas of the network or information that is necessary for them to perform their duties?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Where does the Applicant have a firewall? (check all that apply)		
<input type="checkbox"/> At network perimeter <input type="checkbox"/> Internally within the network to protect sensitive resources		
Which of the following procedures does the Applicant employ to test computer security controls?		
<b>Testing</b>  <input type="checkbox"/> Internal Vulnerability Scanning <input type="checkbox"/> External Vulnerability Scanning against internet-facing IP addresses <input type="checkbox"/> Penetration Testing  <input type="checkbox"/> Other (please describe):	<b>Frequency of Testing</b>  <div style="display: flex; justify-content: space-between;"> <div><input type="checkbox"/> Continuously</div> <div><input type="checkbox"/> Monthly</div> <div><input type="checkbox"/> Quarterly</div> </div> <div style="display: flex; justify-content: space-between;"> <div><input type="checkbox"/> Continuously</div> <div><input type="checkbox"/> Monthly</div> <div><input type="checkbox"/> Quarterly</div> </div> <div style="display: flex; justify-content: space-between;"> <div><input type="checkbox"/> Quarterly</div> <div><input type="checkbox"/> Semi-annually</div> <div><input type="checkbox"/> Annually</div> </div>	
Does the Applicant have network intrusion detection systems that provide actionable alerts if an unauthorized computer system intrusion occurs?		
		<input type="checkbox"/> Yes <input type="checkbox"/> No
If 'Yes', please describe:		
Does the Applicant store data in any of the following environments, and is such stored data encrypted? (check all that apply)		
<input type="checkbox"/> Laptops <input type="checkbox"/> Portable Media <input type="checkbox"/> Back-up Tapes <input type="checkbox"/> "at rest" within computer databases	<div style="display: flex; justify-content: space-between;"> <div><input type="checkbox"/> Encrypted</div> <div><input type="checkbox"/> Not Encrypted</div> </div> <div style="display: flex; justify-content: space-between;"> <div><input type="checkbox"/> Encrypted</div> <div><input type="checkbox"/> Not Encrypted</div> </div> <div style="display: flex; justify-content: space-between;"> <div><input type="checkbox"/> Encrypted</div> <div><input type="checkbox"/> Not Encrypted</div> </div> <div style="display: flex; justify-content: space-between;"> <div><input type="checkbox"/> Encrypted</div> <div><input type="checkbox"/> Not Encrypted</div> </div>	
Does the Applicant outsource any of the following? (Check all that apply and please identify the vendor(s))		
<input type="checkbox"/> Data Center Hosting:	<input type="checkbox"/> Managed Security:	<input type="checkbox"/> Alert Log Monitoring:

**BUSINESS CONTINUITY**

Does the Applicant have :		
A. a disaster recovery plan?	<input type="checkbox"/> Yes <input type="checkbox"/> No	Date last tested:
B. a business continuity plan?	<input type="checkbox"/> Yes <input type="checkbox"/> No	Date last tested:
C. an incident response plan for network intrusions and virus incidents?	<input type="checkbox"/> Yes <input type="checkbox"/> No	Date last tested:
If the Applicant has a business continuity plan, does the plan contain recovery time objectives for the amount of time within which business processes and continuity must be restored?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
If 'Yes', what are the current stated and tested recovery time objectives?		

Does the Applicant have centralized log collection and management that allows for review of all access and activity on the network?	<input type="checkbox"/> Yes <input type="checkbox"/> No
For how long are logs maintained?	
What is Applicant's process for backing up data? (check all that apply)	
<input type="checkbox"/> Full backup <input type="checkbox"/> Incremental <input type="checkbox"/> Differential <input type="checkbox"/> Mirror <input type="checkbox"/> Other:	
How often is Applicant's data backed up?	
Where are data backups stored? (check all that apply) <input type="checkbox"/> Secure offsite <input type="checkbox"/> Secondary Data Center <input type="checkbox"/> Other:	
If necessary, how quickly can backed up data be accessed and restored?	

## MEDIA LIABILITY

Please describe the media activities of the Applicant or by others on behalf of the Applicant	
<input type="checkbox"/> Television <input type="checkbox"/> Radio <input type="checkbox"/> Print <input type="checkbox"/> Applicant's Website(s) <input type="checkbox"/> Internet Advertising <input type="checkbox"/> Social Media <input type="checkbox"/> Marketing Materials <input type="checkbox"/> Audio or Video Streaming	
<input type="checkbox"/> Other (please describe: _____)	
Does the Applicant have a formal review process in place to screen any published or broadcast material (including digital content), for intellectual property and privacy compliance prior to any publication, broadcast, distribution or use?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Are such reviews conducted by, or under the supervision, of a qualified attorney?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Does the Applicant allow user generated content to be displayed on its website(s)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

## E-CRIME

Are all employees that are responsible for disbursing or transmitting funds provided anti-fraud training, including detection of social engineering, phishing, business email compromise, and other scams on at least an annual basis?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Before processing fund transfer requests from internal sources, does the Applicant confirm the instructions via a method other than the original means of the instruction?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Do the Applicant's procedures require review of all requests by a supervisor or next-level approver before processing fund transfer instructions?	<input type="checkbox"/> Yes <input type="checkbox"/> No
When a vendor/supplier requests any change to its account details (including routing numbers, account numbers, telephone numbers and contact information) and prior to making any changes:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the Applicant first confirm all requested changes requested by the vendor/supplier with a person other than the requestor prior to making any changes?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the Applicant confirm requested changes via a method other than the original means of request?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Do the Applicant's processes and procedures require review of all requests by a supervisor or next-level approver?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Please identify your telecommunications carrier:

Have you established strong alphanumeric passwords for administrative controls of your telecommunications system?

☐ Yes ☐ No

Have you configured your telecommunications system to disable (check all that apply):

☐ Remote system administration and Internet Protocol (IP) access ☐ Dialing via remote system access (DISA)

### PRIOR CLAIMS AND CIRCUMSTANCES

Does the Applicant or other proposed insured (including any director, officer or employee) have knowledge of or information regarding any fact, circumstance, situation, event or transaction which may give rise to a claim, loss or obligation to provide breach notification under the proposed insurance?

☐ Yes ☐ No

If yes, please provide details:

During the past five (5) years has the Applicant:

a. received any claims or complaints with respect to privacy, breach of information or network security, or, unauthorized disclosure of information?

☐ Yes ☐ No

b. been subject to any government action, investigation or subpoena regarding any alleged violation of a privacy law or regulation?

☐ Yes ☐ No

c. received a complaint or cease and desist demand alleging trademark, copyright, invasion of privacy, or defamation with regard to any content published, displayed or distributed by or on behalf of the Applicant?

☐ Yes ☐ No

d. notified consumers or any other third party of a data breach incident involving the Applicant?

☐ Yes ☐ No

e. experienced an actual or attempted extortion demand with respect to its computer systems?

☐ Yes ☐ No

f. experienced an unexpected outage of a computer network, application or system lasting greater than four (4) hours?

☐ Yes ☐ No

If 'Yes' to any of the above, please provide details regarding such incident(s) or event(s):

THE UNDERSIGNED IS AUTHORIZED BY THE APPLICANT TO SIGN THIS APPLICATION ON THE APPLICANT'S BEHALF AND DECLARES THAT THE STATEMENTS CONTAINED IN THE INFORMATION AND MATERIALS PROVIDED TO THE INSURER IN CONJUNCTION WITH THIS APPLICATION AND THE UNDERWRITING OF THIS INSURANCE ARE TRUE, ACCURATE AND NOT MISLEADING. SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE INSURER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THE STATEMENTS CONTAINED IN THIS APPLICATION AND ANY OTHER INFORMATION AND MATERIALS SUBMITTED TO THE INSURER IN CONNECTION WITH THE UNDERWRITING OF THIS INSURANCE ARE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED, AND HAVE BEEN RELIED UPON BY THE INSURER IN ISSUING ANY POLICY.

THIS APPLICATION AND ALL INFORMATION AND MATERIALS SUBMITTED WITH IT SHALL BE RETAINED ON FILE WITH THE INSURER AND SHALL BE DEEMED ATTACHED TO AND BECOME PART OF THE POLICY IF ISSUED. THE INSURER IS AUTHORIZED TO MAKE ANY INVESTIGATION AND INQUIRY AS IT DEEMS NECESSARY REGARDING THE INFORMATION AND MATERIALS PROVIDED TO THE INSURER IN CONNECTION WITH THE UNDERWRITING AND ISSUANCE OF THE POLICY.

THE APPLICANT AGREES THAT IF THE INFORMATION PROVIDED IN THIS APPLICATION OR IN CONNECTION WITH THE UNDERWRITING OF THE POLICY CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE

EFFECTIVE DATE OF THE INSURANCE, THE APPLICANT WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE INSURER OF SUCH CHANGES, AND THE INSURER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE.

I HAVE READ THE FOREGOING APPLICATION FOR INSURANCE AND REPRESENT THAT THE RESPONSES PROVIDED ON BEHALF OF THE APPLICANT ARE TRUE AND CORRECT.

**FRAUD WARNING DISCLOSURE**

**ANY PERSON WHO, WITH INTENT TO DEFRAUD OR KNOWING THAT (S)HE IS FACILITATING A FRAUD AGAINST THE INSURER, SUBMITS AN APPLICATION OR FILES A CLAIM CONTAINING A FALSE OR DECEPTIVE STATEMENT MAY BE GUILTY OF INSURANCE FRAUD.**

**NOTICE TO ALABAMA, ARKANSAS, LOUISIANA, NEW MEXICO AND RHODE ISLAND 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 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 COMMITS A FRAUDULENT INSURANCE ACT.

**NOTICE TO KENTUCKY, NEW JERSEY, NEW YORK, 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 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 SUBJECTS SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES. (IN NEW YORK, THE CIVIL PENALTY IS NOT TO EXCEED FIVE THOUSAND DOLLARS (\$5,000) AND THE STATED VALUE OF THE CLAIM FOR EACH SUCH VIOLATION.)

**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 MAY INCLUDE IMPRISONMENT, FINES OR A 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 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 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.

#### **SIGNATURE SECTION**

THE UNDERSIGNED AUTHORIZED EMPLOYEE OF THE APPLICANT DECLARES THAT THE STATEMENTS SET FORTH HEREIN ARE TRUE. THE UNDERSIGNED AUTHORIZED EMPLOYEE AGREES THAT IF THE INFORMATION SUPPLIED ON THIS APPLICATION CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, HE/SHE WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE UNDERWRITER OF SUCH CHANGES, AND THE UNDERWRITER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE. FOR NEW HAMPSHIRE APPLICANTS, THE FOREGOING STATEMENT IS LIMITED TO THE BEST OF THE UNDERSIGNED'S KNOWLEDGE, AFTER REASONABLE INQUIRY. IN MAINE, THE UNDERWRITERS MAY MODIFY BUT MAY NOT WITHDRAW ANY OUTSTANDING QUOTATIONS OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE.

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. NO COVERAGE SHALL BE AFFORDED FOR ANY CLAIMS ARISING OUT OF A CIRCUMSTANCE NOT DISCLOSED IN THIS APPLICATION.

SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE UNDERWRITER 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 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. FOR NORTH CAROLINA, UTAH, AND WISCONSIN APPLICANTS, SUCH APPLICATION MATERIALS ARE PART OF THE POLICY, IF ISSUED, ONLY IF ATTACHED AT ISSUANCE.

Signed\*:\_\_\_\_\_

Date:\_\_\_\_\_

Print Name:\_\_\_\_\_

Title: \_\_\_\_\_

If this **Application** is completed in Florida, please provide the Insurance Agent's name and license number. If this **Application** is completed in Iowa or New Hampshire, please provide the Insurance Agent's name and signature only.

Agent's Signature\*:\_\_\_\_\_

Agent's Printed Name:\_\_\_\_\_

Florida Agent's License Number:\_\_\_\_\_



# Ransomware Supplemental Application

Please provide responses below concerning the Information Technology (IT) environment of your organization and any subsidiaries for which the insurance is being sought.

**Responses to this application should be accurate as of the date that the application is signed and dated below.** If your organization plans to make changes to its IT environment prior to inception of the policy, or during the policy period, please describe those plans in the "Other Cybersecurity Controls & Preventative Measures" section, below.

## Budgets & Personnel

1. a. Annual IT budget \$ \_\_\_\_\_ b. Percentage of IT budget spent on cybersecurity \_\_\_\_\_%
2. a. Full-time IT employees \_\_\_\_\_ b. Full-time IT cybersecurity employees \_\_\_\_\_
3. Cybersecurity point of contact (CISO or equivalent role):

Name	Title	Email	Telephone
------	-------	-------	-----------

## Email Security

4. What security controls do you have in place for incoming email? Choose all that apply.
 

a. <input type="checkbox"/> Screening for malicious attachments	e. <input type="checkbox"/> Tagging external emails
b. <input type="checkbox"/> Screening for malicious links	f. <input type="checkbox"/> DomainKeys Identified Mail (DKIM)
c. <input type="checkbox"/> Quarantine service	g. <input type="checkbox"/> Sender Policy Framework (SPF) strictly enforced
d. <input type="checkbox"/> Detonation and evaluation of attachments in a sandbox	h. <input type="checkbox"/> Domain Based Message Authentication, Reporting and Conformance (DMARC)

5. How frequently do you conduct the following training for all employees?

Type of training	Never/not regularly	Annually	≥2x per year
a. Interactive phishing training	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b. Phishing email simulations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

6. Do you require additional training for employees who fail phishing email simulations? ☐ No ☐ Yes
7. a. What Microsoft 365 license (or equivalent license) do you use for all, or substantially all, of your users? ☐ E1 ☐ E3 ☐ E5 ☐ Other ☐ None
   
b. If you use Microsoft 365, do you use the Microsoft 365 Defender (formerly known as Advanced Threat Protection) add-on or an equivalent cybersecurity product with advanced threat hunting? (Leave blank if you do not use Microsoft 365.) ☐ No ☐ Yes
8. a. Do you disable macros in your office productivity software by default? (E.g., Microsoft Office, Google Workspace) ☐ No ☐ Yes
   
b. If "Yes" to a., are users allowed to enable macros? ☐ No ☐ Yes
9. Have you disabled legacy email protocols that use basic authentication (a username and password only), such as IMAP, POP3, and SMTP? ☐ No ☐ Yes



## Identity & Access Management

10. Do you enforce multi-factor authentication (MFA) for all user accounts (other than Domain Administrator accounts) when accessing your network remotely? Please note any exceptions in the "Other Cybersecurity Controls & Preventative Measures" section, below.

☐ No ☐ Yes ☐ Remote access not permitted

MFA includes but is not limited to the following: a call, SMS, push notification, time-based one-time password, OATH token, hardware token, device pinning, authenticator apps, biometrics, or a FIDO2 key (e.g., YubiKey, RSA SecurID).

"User accounts" include employees and (where applicable) students, volunteers, interns, third-party contractors, and any other persons with a user account on your network; "user accounts" does not include service accounts, which are addressed in a separate section below.

11. a. Do you permit users remote access to web-based email (e.g., Outlook Web Access (OWA))? ☐ No ☐ Yes  
 b. If "Yes" to a., do you enforce MFA for access to web-based email? ☐ No ☐ Yes
12. Do you provide your employees with password management software? ☐ No ☐ Yes
13. Do you enforce MFA for all Domain Administrator accounts? Please note any exceptions in the "Other Cybersecurity Controls & Preventative Measures" section, below. "Domain Administrator accounts" does not include service accounts, which are addressed in a separate section below. ☐ No ☐ Yes
14. Do you permit ordinary users local administrator rights to their devices (e.g., laptops)? ☐ No ☐ Yes
15. a. Do you use a Privileged Access Management (PAM) tool? ☐ No ☐ Yes  
 b. If "Yes" to a., are all privileged accounts managed with a PAM tool? ☐ No ☐ Yes

## Unsupported & End of Life Software

16. Do you use an asset discovery tool that continuously maps devices on your internal network? ☐ No ☐ Yes
17. Do you have an up-to-date asset database? ☐ No ☐ Yes
18. Do you have an up-to-date configuration management database (CMDB)? ☐ No ☐ Yes
19. a. Do you have any end-of-life or end-of-support software on your network? ☐ No ☐ Don't know ☐ Yes  
 b. If "Yes" to a., is the software segregated from the rest of the network?  
☐ No ☐ Some is, some isn't ☐ Yes  
 c. If "Yes" to a., do you purchase additional support for the software, where available? ☐ No ☐ Yes

## Service Accounts

20. How many service accounts with domain administrator privileges are in your IT environment? "Service accounts" are non-human privileged accounts used to execute applications, access local and network resources, and run automated services, virtual machine instances, and other processes.

☐ >10 ☐ 6-10 ☐ 1-5 ☐ 0

*Please answer the remaining questions in this section only with respect to service accounts with domain administrator privileges. If you do not have any service accounts with domain administrator privileges, please skip the remaining questions in this section.*

21. Do you configure service accounts using the principle of least privilege? (I.e., have you removed domain administrator privileges from those service accounts that don't require such privileges to function?) ☐ No ☐ Yes
22. Do you have specific monitoring rules in place for service accounts to alert your Security Operations Center (SOC) of any abnormal behavior? ☐ No ☐ Yes
23. Have you configured service accounts to deny interactive logins? ☐ No ☐ Yes
24. Do you require service account passwords to be ≥25 characters or to be randomly generated? ☐ No ☐ Yes
25. Do you rotate passwords for service accounts on a regular basis? ☐ No ☐ Yes
26. Do you manage passwords for service accounts with a PAM solution or password vault? ☐ No ☐ Yes

## Security Products & Solutions

27. What security solutions do you use to prevent or detect malicious activity on your network?

Security solution	Vendor
a. Endpoint Protection Platform (EPP)	
b. Endpoint Detection and Response (EDR)	
c. Managed Detection and Response (MDR)	
d. Network Detection and Response (NDR)	
e. Security Information and Event Management (SIEM)	
f. Application Isolation and Containment	

28. a. Do you have a Security Operations Center (SOC)? ☐ No ☐ Yes, working hours only ☐ Yes, 24/7
- b. If "Yes" to a., is your SOC internal or managed by a third party? ☐ Internal ☐ Third party ☐ Both
- c. If "Yes" to a., does your SOC have the authority and ability to remediate security events (for example, by isolating and containing endpoints remotely)? ☐ No ☐ Yes
29. Do you use a protective DNS service (e.g., Quad9, OpenDNS or the public sector PDNS)? ☐ No ☐ Yes
30. Are host-based and network firewalls configured to disallow inbound connections by default? ☐ No ☐ Yes
31. a. Do you use Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), AnyDesk, TeamViewer, or other remote desktop software? ☐ Yes ☐ Yes, but internally only and not exposed to the internet ☐ No
- b. If "Yes" to a., does access require MFA? ☐ No ☐ Yes
32. Do you deny all Server Message Block (SMB) (i.e., Windows file sharing) inbound communications to servers (except where there is an identified business need)? ☐ No ☐ Yes

## Vulnerabilities & Scanning

33. Do you use a hardened baseline configuration across all (or substantially all) of your devices? ☐ No ☐ Yes
34. What percentage of the enterprise is covered by scheduled vulnerability scans? \_\_\_\_\_ %
35. In the past two years, how often have you conducted vulnerability scanning of the devices on your network?
- ☐ Never/not regularly ☐ Annually ☐ 2-3 times per year ☐ Quarterly or more often

36. In the past two years, what is the average time that your organization has taken to remediate Critical Common Vulnerabilities and Exposures (Critical CVEs) (CVSS version 3.1 Base Score 9.0-10.0) on your network?

☐ Unknown ☐ >2 weeks ☐ <2 weeks ☐ <1 week ☐ <48 hours

37. How often do you (or a third party on your behalf) conduct penetration testing on your network?

☐ Never/not regularly ☐ Annually ☐ 2-3 times per year ☐ Quarterly or more often

## Backups & Resilience

38. Do you rely on a backup solution that is located on your corporate network? ☐ No ☐ Yes

39. a. Do you rely on a cloud-based service as your backup location? ☐ No ☐ Yes

b. If "Yes" to a., is your cloud-based backup service a "syncing service"?  
(E.g., DropBox, OneDrive, SharePoint, Google Drive) ☐ No ☐ Yes

c. If "Yes" to a., have you determined how long it would take to restore all of your data from the cloud?  
☐ No ☐ Yes, >1 week ☐ Yes, >48 hours but <1 week ☐ Yes, <48 hours

40. Do you maintain any offline backups? ☐ No ☐ Yes, partial backups ☐ Yes, full backups

41. a. Are all of your backups encrypted? ☐ No ☐ Some backups are encrypted, some aren't ☐ Yes

b. For your encrypted backups, do you maintain an offline backup of your decryption key(s)? ☐ No ☐ Yes  
(Skip this question if you do not have any encrypted backups.)

42. Are any of your backup solutions "immutable"? (Immutable backups cannot be altered or deleted.) ☐ No ☐ Yes

43. How frequently do you perform a test restoration from backups?  
☐ Never/not regularly ☐ Annually ☐ 2-3 times per year ☐ Quarterly or more often

44. Do you have the ability to test the integrity of backups prior to restoration to be confident that your backups are free from malware? ☐ No ☐ Yes

## Business Continuity & Planning

45. a. Do you have a business continuity or disaster recovery plan, that includes responding to cybersecurity threats, that was created or updated within the past two years? ☐ No ☐ Yes

b. If "Yes" to a., have you engaged in any exercises to run through the plan (from start to finish) with your incident response team? ☐ No ☐ Yes

46. a. Have you conducted, within the past two years, a cybersecurity incident tabletop exercise? ☐ No ☐ Yes

b. If "Yes" to a., did that tabletop exercise include the threat from ransomware? ☐ No ☐ Yes

## Other Cybersecurity Controls & Preventative Measures

Please use the space below to clarify any answers above that may be incomplete or require additional detail. Please also describe any additional steps your organization takes to detect, prevent, and recover from ransomware attacks (e.g., segmentation of your network, additional software security controls, external security services, etc.).



THE UNDERSIGNED IS AUTHORIZED BY THE APPLICANT TO SIGN THIS APPLICATION ON THE APPLICANT'S BEHALF AND DECLARES THAT THE STATEMENTS CONTAINED IN THE INFORMATION AND MATERIALS PROVIDED TO THE INSURER IN CONJUNCTION WITH THIS APPLICATION AND THE UNDERWRITING OF THIS INSURANCE ARE TRUE, ACCURATE AND NOT MISLEADING. SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE INSURER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THE STATEMENTS CONTAINED IN THIS APPLICATION AND ANY OTHER INFORMATION AND MATERIALS SUBMITTED TO THE INSURER IN CONNECTION WITH THE UNDERWRITING OF THIS INSURANCE ARE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED, AND HAVE BEEN RELIED UPON BY THE INSURER IN ISSUING ANY POLICY.

THIS APPLICATION AND ALL INFORMATION AND MATERIALS SUBMITTED WITH IT SHALL BE RETAINED ON FILE WITH THE INSURER AND SHALL BE DEEMED ATTACHED TO AND BECOME PART OF THE POLICY IF ISSUED. THE INSURER IS AUTHORIZED TO MAKE ANY INVESTIGATION AND INQUIRY AS IT DEEMS NECESSARY REGARDING THE INFORMATION AND MATERIALS PROVIDED TO THE INSURER IN CONNECTION WITH THE UNDERWRITING AND ISSUANCE OF THE POLICY.

THE APPLICANT AGREES THAT IF THE INFORMATION PROVIDED IN THIS APPLICATION OR IN CONNECTION WITH THE UNDERWRITING OF THE POLICY CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, THE APPLICANT WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE INSURER OF SUCH CHANGES, AND THE INSURER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE.

I HAVE READ THE FOREGOING APPLICATION FOR INSURANCE AND REPRESENT THAT THE RESPONSES PROVIDED ON BEHALF OF THE APPLICANT ARE TRUE AND CORRECT.

***Digital signature required below [click the red tab to create a digital ID or import an existing digital ID]:***

Signed: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Company: \_\_\_\_\_

Date: \_\_\_\_\_

**Instructions for Using Editable Applications and Important Legal Information:**

**This is a static sample document for demonstration / discussion purposes only. This not intended to represent a current version of an application; please do not use it for actual form submittal.**

1. Save the document to your local computer.
2. Complete the application by providing your responses in the areas provided; utilize the tab key to move ahead to the next field.
3. If there is not enough space for any particular question, please include the full response in an additional attachment to your application, as you would if you were completing a paper-based application.
4. When you have completed the application, please verify the application for accuracy and completeness before signing the application and forwarding the application to your agent or broker. Do not forward applications directly to Chubb unless you are an agent or broker.
5. If you choose to sign the application with a wet signature, please print the final application, sign the application in ink and forward the application to your agent or broker with any necessary supporting materials.
6. If you apply your signature to this form electronically, you hereby consent and agree that your use of a key pad, mouse or other device to click the "I Agree" button constitutes your signature, acceptance and agreement as if actually signed by you in writing and has the same force and effect as a signature affixed by hand. Further, you agree that the lack of a certification authority or other third party verification will not in any way affect the validity or enforceability of your signature or any resulting contract. You can apply your signature electronically by clicking on the signature field. Once all signatures have been applied, forward the application to your agent or broker via email. Any necessary supporting materials should be sent via email or postal service to your agent or broker.

If you experience technical difficulties utilizing the document, please contact the Chubb Help Desk at 1-877-747-5266, "Option 2".  
For all other inquiries please contact your agent or broker. If you are an agent or broker, please contact your local Chubb representative. The document is provided for licensed insurance agents and brokers and their clients only.

**IF YOU ARE ACCESSING THE DOCUMENT FROM A VENUE OTHER THAN WWW.CHUBB.COM, BY YOUR USE OF THE DOCUMENT, YOU ARE AGREEING TO THE FOLLOWING, IF YOU DO NOT AGREE, DO NOT USE THE ELECTRONIC DOCUMENT:**

- \* Chubb does not warrant that the document will be free from viruses. You assume the entire cost of any necessary service, repair or correction.
- \* The privacy of communication over the Internet cannot be guaranteed, because the Internet is not a secure medium. Chubb does not assume any responsibility for any harm, loss, or damage you may experience or incur by the sending of personal or confidential information over the Internet.
- \* Chubb is not responsible for any versions of the document that have been manipulated, altered or revised from the version of the document that appears on www.Chubb.com. Do not post the document on the Internet.

"Chubb" refers to the member insurers of the Chubb Group of Insurance Companies, Copyright notice: All rights reserved.

**I Agree**

notices and information regarding the proposed policy):

Name: \_\_\_\_\_ e-Mail: \_\_\_\_\_

Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_ Telephone: \_\_\_\_\_

**II. INSURANCE INFORMATION:**

1. Indicate below which coverages are being requested by indicating requested limits and deductibles or retentions. If coverage is currently purchased, indicate current limits, deductibles or retentions and carrier. If coverage is currently not purchased, please so indicate.

Coverage Requested	Limit of Liability Requested	Limit of Liability Currently Purchased	Deductible or Retention Requested	Deductible or Retention Currently Purchased	Current Insurer	Retro Date of Current Policy
Coverage A - Errors and Omissions Liability Coverages (Select one)						
Technology Products & Services						
Coverage B - Destructive Programming						
Destructive Programming					N/A	N/A



Coverage Requested	Limit of Liability Requested	Limit of Liability Currently Purchased	Deductible or Retention Requested	Retention Currently Purchased	Current Insurer	Retro Date of Current Policy
Coverage C - Cyber Liability Coverage (Select the coverages being requested)						
Cyber Liability						
Consumer Redress Fund						
Coverage D – Intellectual Property Infringement, Disclosure of Confidential Information and Reputation Disparagement						
Intellectual Property Infringement						
Disclosure of Confidential Information						
Reputation Disparagement						

Additional Coverage Requested	Limit of Insurance Requested	Limit of Insurance Currently Purchased	Deductible or Retention Requested	Retention Currently Purchased
Additional Coverage - Basket Limit (Options include \$100,000,\$250,000.or \$500,000).				
Privacy Remediation Expenses				
Cyber-Threat Expenses				
Optional Additional Coverages				
Cyber-Reward				
Confidential Breach Expenses				
Fines and Penalties				
Impairment of Computer Services(e.g. business income, Extra Expense and Data Recovery Costs)				
Optional Additional Specific Limits of Insurance for Additional Coverages	Limit of Insurance Requested	Limit of Insurance Currently Purchased	Deductible or Retention Requested	Retention Currently Purchased
Privacy Remediation Expenses Aggregate Limit				
“Notification Expenses”				
“Forensics Expenses”				
“Remediation Expenses”				
“Regulatory Expenses”				

2. Policy Period Requested:  
From \_\_\_\_\_ to \_\_\_\_\_ both days at 12:01 a.m. at the principal address of the Parent Organization.

**III. GENERAL RISK INFORMATION:**

1. Provide your legal structure: \_\_\_\_\_
2. Year established: \_\_\_\_\_ State of Incorporation: \_\_\_\_\_ Primary SIC Code: \_\_\_\_\_
3. Description of business operations: \_\_\_\_\_
4. During the past two years you completed 3 or more acquisitions? ☐ Yes ☐ No

5. Complete the following information:

	Prior Fiscal Year	Current Fiscal Year Annualized Projection	Projected (Next) Fiscal Year
i. Number of Employees			
ii. Gross Revenue			
iii. Gross Payroll			

(a) Advise the percentage of prior fiscal year gross revenues derived outside the United States: \_\_\_\_\_%

6. What is the highest gross revenue of any customer to whom you have or will provide products or services to in the past three years? ☐ < \$250mm ☐ Between \$250mm and \$1Bn ☐ > \$1Bn

7. Does Applicant maintain general liability insurance for the purchase of bodily injury, property damage, personal injury and advertising injury coverage, including products-completed operations insurance? ☐ Yes ☐ No

If "Yes", indicate whether:

(a) Professional liability exposures are excluded ☐ Yes ☐ No

(b) Security Breach; access or disclosure of personal information are excluded ☐ Yes ☐ No

#### IV. COVERAGE SPECIFIC RISK INFORMATION:

##### A. OPERATIONAL ANALYSIS, POLICIES AND PROCEDURES (APPLICABLE TO ALL APPLICANTS)

1. Do you collect, store or process personally identifiable or other confidential information (see listed in (b) below)? ☐ Yes ☐ No

If "Yes":

(a) How many records are held, including but not limited to prospective, current and former customers, business partners and employees? \_\_\_\_\_

(b) Check all forms of personally identifiable or confidential information that apply:

- |  |   |   |
|--|---|---|
| <input type="checkbox"/> Credit Card Information | <input type="checkbox"/> Financial Information  | <input type="checkbox"/> Personal Information |
| <input type="checkbox"/> Customer Information    | <input type="checkbox"/> Healthcare Information | <input type="checkbox"/> Trade Secrets        |
| <input type="checkbox"/> Other                   |   |   |

2. Have you implemented a written information security policy which is applicable to all of your business units? ☐ Yes ☐ No

If "Yes":

(a) Do you test the security required by the security policy at least annually? ☐ Yes ☐ No

(b) Do you regularly identify and assess new threats and vulnerabilities and adjust the security accordingly? ☐ Yes ☐ No

(c) Does your information security policy include policies for the use and storage of personally identifiable or other confidential information on mobile devices? ☐ Yes ☐ No

(d) Does your information security policy identify the threats and vulnerabilities and adjust accordingly pertaining to your Industrial Control Systems? ☐ Not applicable ☐ Yes ☐ No



3. Check whether your information security policies include the following:
- |   |   |   |
|---|---|---|
| <input type="checkbox"/> Fire walls to filter all traffic     | <input type="checkbox"/> Regularly scheduled patch management process         | <input type="checkbox"/> Use of Penetration and Vulnerability Scans   |
| <input type="checkbox"/> Authentication and Access Lists      | <input type="checkbox"/> Encryption used on data at rest and in transit       | <input type="checkbox"/> Annual employee and authorized user training |
| <input type="checkbox"/> Enterprise use of Anti-virus program | <input type="checkbox"/> Access revocation following termination or departure | <input type="checkbox"/> Use of Intrusion Detection                   |
4. Do you have a Business Continuity and Disaster Recovery Plan? ☐ Yes ☐ No
- If "Yes":
- (a) Is the Plan reviewed and updated at least bi-annually? ☐ Yes ☐ No
- (b) Is the Plan tested at least annually? ☐ Yes ☐ No
- (c) Have any problems identified in review or testing been rectified? ☐ Yes ☐ No
- (d) How long would it take to restore operations after a computer attack or other Loss/corruption of data?
- ☐ No Interruption ☐ < 48 hours ☐ Between 48 and 96 Hours ☐ > 96 hours
5. Do you have a written incident response plan that addresses network security incidents or privacy threats? ☐ Yes ☐ No
6. How frequently do you back up electronic data?
- ☐ Daily with multi-generations retained ☐ Daily ☐ Less than daily
7. Do you employ a designated security officer or equivalent (CSO/CISO)? ☐ Yes ☐ No
- If "No", who within the organization has been designated to manage and implement information security policies, procedures and processes \_\_\_\_\_
8. Do you currently use, or have plans in the next year to use, the services of a cloud service or other outsourced service provider? ☐ Yes ☐ No
- If "Yes", complete the following:
- (a) What impact would an interruption or cessation of such services have on **Applicant's** ability to meet customer contractual obligations? ☐ None ☐ Slight ☐ Significant
- (b) Does **Applicant's** disaster recovery or business continuity plan specifically address restoration and recovery of business operations provided by a cloud service provider? ☐ Yes ☐ No
9. Do you have formalized process when privileged access (e.g. administrator level) is granted? If "Yes": ☐ Yes ☐ No
- (a) Privileged Access is granted on need only (least privileged) basis ☐ Yes ☐ No
- (b) Subject to continuous technological, operational and security review; audit and process improvement. ☐ Yes ☐ No

**B. TECHNOLOGY PRODUCTS AND SERVICES COVERAGE (Complete if requesting Coverage A.)**

**Products, Services and Industries Served**

1. Are your products sold directly to or your services offered directly to consumers? ☐ Yes ☐ No
2. Do you presently offer 10 or more distinctive products or services? ☐ Yes ☐ No
3. Have you discontinued any products or services in the past three years? ☐ Yes ☐ No
- If "Yes", do you continue to provide service or maintenance? ☐ Yes ☐ No
4. Do you have any products or services entering new markets or territories within the next year that are substantially different in scope or end use than current products or services? ☐ Yes ☐ No

5. **Technology Customers** - Complete the table below and answer the questions that immediately follow.

Types of Products & Services	Industries Served	Projected (Next) Fiscal Year
Hardware Assembly		
Hardware Component Manufacturing		
Prepackaged Software/Value Added Resellers		
Data Processing		
Consulting		
Custom Software/System Integration		
Network Hardware Manufacturing		
Network Transport		
Network Services		
Network Services, including System Integration		

- (a) Indicate the projected next fiscal year revenue derived from:

Type	Projected (Next) Fiscal Year
Software as a Service (SaaS)	
Infrastructure as a Service (IaaS)	
Platform as a Services (PaaS)	
Total	

- (b) Check if you offer any of the following products or services:

- ☐ Used or incorporated into any automobile aircraft, watercraft or transportation product or equipment
 ☐ Credit Card or Payment-Processing Services
 ☐ Consumer profiling or surveillance products or services
 ☐ Data or Content Retrieval or Aggregation
- ☐ Direct to consumer information security software
 ☐ Services to intelligence agencies or departments
 ☐ Auction, File-Sharing or Social-Networking Web Site
 ☐ Enterprise Retail Merchant Services
- ☐ Business Processing Outsourcing
 ☐ Health Information Exchange (HIE's)
 ☐ Mobile Application Developer
 ☐ Mobile Phones
- ☐ Security Consulting

6. Are licensed professionals (e.g. architects, attorneys or physicians) required to fulfill your contractual obligations? ☐ Yes ☐ No

If "Yes":

- (a) Describe the services provided by such Professionals \_\_\_\_\_

- (b) Do you currently purchase stand-alone professional liability insurance? ☐ Yes ☐ No

Carrier: \_\_\_\_\_ Policy Period from \_\_\_\_\_ to \_\_\_\_\_

7. In delivery of your products or provisioning of your services, are you dependent upon third parties to provide raw materials, components or final products? ☐ Yes ☐ No

If one or more, do any represent 25% or more of your gross revenues? ☐ Yes ☐ No

If "Yes": describe 3<sup>rd</sup> party suppliers who represent 25% or greater in revenue:

8. What would be the largest financial and business impact on customers from a failure of any of your products or services? ☐ No disruption ☐ Minor or delayed ☐ Major or immediate  
If other than "No disruption", describe impact on confidentiality, integrity and availability of data: \_\_\_\_\_
9. Do you engage subcontractors or other third parties to provide development, implementation, maintenance or support services? ☐ Yes ☐ No  
(a) What percentage of services are subcontracted \_\_\_\_\_%  
(b) Do you require subcontractors to carry their own E&O insurance? ☐ Yes ☐ No  
(c) Do you contractually require indemnification from subcontractors? ☐ Yes ☐ No  
(d) Describe services subcontracted to others: \_\_\_\_\_
10. Do you have a process evaluate current and prospective customers, subcontractors and suppliers? ☐ Yes ☐ No  
If "Yes":  
(a) Does this process include evaluating financial condition? ☐ Yes ☐ No  
(b) Does this process include evaluating ability to fulfill their commercial and contractual obligations? ☐ Yes ☐ No
11. Do you derive revenue from performing fee based services to on customer specifications? ☐ Yes ☐ No  
If "Yes": indicate the percentage below:  
☐ less than 50%  
☐ between 50% and 90%  
☐ greater than 90%

**C. Customer Contract & Project Management**

1. Do you use a written agreement (e.g., contract, engagement letter, sales agreement, purchase order) with clients? ☐ Always ☐ Sometimes ☐ Never
2. Do you have stated minimum contract standards, including any non-disclosure and confidentiality agreements? ☐ Yes ☐ No
3. Do your global contracts or agreements comply with stated minimum standards? ☐ Yes ☐ No
4. Do your contracts and agreements include limitation of liability provisions that extend to actual or alleged breach or potential breach of personal information? ☐ Yes ☐ No
5. Do you contractually assume the obligations to notify affected persons or organizations following an actual data breach? ☐ Yes ☐ No
6. Do you have a process to ensure that your data and information security policies comply with system and data access agreements from entities that provide you products or services (e.g. financial institutions, cloud service providers or benefit administrator)? ☐ Yes ☐ No  
Indicate whether such contracts or agreements include:  
(a) Your right to verify that recipient of your data is complying with the data security and integrity obligations set forth the contract or agreement ☐ Yes ☐ No  
(b) The recipient's rights to verify that you are complying with the data security and integrity obligations set forth in the contract or agreement ☐ Yes ☐ No  
(c) Contractual cures and remedies exits in cases of non-compliance ☐ Yes ☐ No
7. Do you accept customers' customized contracts, purchase orders or agreements? ☐ Yes ☐ No  
If "Yes":  
(a) Does legal counsel or senior management review all such contracts, purchase orders or agreements prior to execution? ☐ Yes ☐ No

- (b) What % of the time, do accept customers' customized contracts, purchase orders or agreements?  
☐ Less than 15%    ☐ Between 15-33    ☐ More than 33%

8. Indicate whether your contract and project management procedures include the following:

- (a) A written proposal or request for information in order to determine customer performance expectations ☐ Yes ☐ No
- (b) A written contract of specifications of products and services you will provide, signed by the customer ☐ Yes ☐ No
- (c) A document outlining the responsibilities of all parties ☐ Yes ☐ No
- (d) A document outlining the scope of the project or services ☐ Yes ☐ No
- (e) Interim changes documented with customer sign-off ☐ Yes ☐ No
- (f) Performance milestones acknowledged and accepted with customer sign-off when achieved ☐ Yes ☐ No
- (g) Physical and electronic measures to safeguard customer content, information or material received pursuant to the terms and conditions of all non-disclosure and confidentiality agreements ☐ Yes ☐ No
- (h) Formal patch issuance program for your customers ☐ Yes ☐ No

9. What is the most common value of your average performance-based contract, purchase order or agreement?

10. What is the duration, in months, of your most common performance-based contract, purchase order or agreement?

11. Provide the following information for the five largest contracts, purchase orders or agreements excluding ongoing service and maintenance revenue:

Customer	Annual Revenue	Contract Amount	Contract Duration	Product or Service

12. Do you require contractual indemnifications and appropriate insurance (E & O, Professional Indemnity or Cyber) when granting computer access to a third party? ☐ Yes ☐ No

#### D. Quality Control

1. Indicate whether your quality control procedures include the following:

- (a) Written and formalized quality-control program ☐ Yes ☐ No
- (b) Alpha testing ☐ Yes ☐ No
- (c) Beta testing ☐ Yes ☐ No
- (d) Formal customer-acceptance procedure ☐ Yes ☐ No
- (e) Systems-development methodology in writing ☐ Yes ☐ No
- (f) Formal product-recall plan ☐ Yes ☐ No
- (g) Formal policy for documenting and responding to customer complaints or requests for changes or fixes ☐ Yes ☐ No
- (h) Use of tools (e.g, static analyzers) or other forensic methodologies to assist in identifying code vulnerabilities ☐ Yes ☐ No

2. Indicate whether your products or services comply with any of the following accepted industry standards:  
☐ IEEE ☐ ANSI ☐ CE Mark ☐ UL/CSA ☐ ASTM Other(s): \_\_\_\_\_
3. Do all developers receive training on best practices and techniques for writing secure applications? ☐ N/A (does not develop software or firmware) ☐ Yes ☐ No  
If "Yes"; indicate whether:  
(a) Developers receive training Secure Development Lifecycle (SDL), including best practices for writing secure applications ☐ Yes ☐ No  
(b) Developers use threat modeling to assess the risks and vulnerabilities ☐ Yes ☐ No
4. Do you have a formalized process to ensure that all products or services are continually evaluated throughout their life cycle for known and latent (security) vulnerabilities? ☐ Yes ☐ No  
If "Yes": \_\_\_\_\_  
(a) Prior to release and throughout the product lifecycle do you have a methodology to communicate vulnerabilities and remedies; e.g. interim patches? ☐ Yes ☐ No
5. Do you have a document-retention policy addressing all business functions? ☐ Yes ☐ No

**E. Training, Support & Dispute Resolution**

1. Does legal counsel review all external product, sales and marketing material prior to publication and use? ☐ Yes ☐ No
2. Do you conduct formal sales and marketing training for employees and third party vendors engaged in the sale, service or distribution of your products and services? ☐ Yes ☐ No
3. Indicate whether you:  
(a) Provide at least two forms of customer or product support ☐ Yes ☐ No  
(b) Offer customer support 24 hours a day ☐ Yes ☐ No  
(c) Maintain written logs for customer complaints of problems or downtime ☐ Yes ☐ No  
If "Yes", how long are they retained? (number of whole or partial months) \_\_\_\_\_  
(d) Has an formal escalation procedure for unresolved issues greater than 30 days in duration ☐ Yes ☐ No
4. Do you have any contracts currently past due? ☐ Yes ☐ No
5. Have you experienced any contract disputes within the past five years? ☐ Yes ☐ No  
If "Yes", have any customers withheld payment or requested a refund as a result of a contract dispute within the past three years? ☐ Yes ☐ No

**F. Intellectual Property, Disclosure of Confidential Information and Reputation Disparagement**

1. Do your intellectual property management policies include the following:  
(a) Copyright and trademark searches conducted by qualified legal counsel or a professional search firm, which include looking for your domain name and product/service designs, names or logos. ☐ Yes ☐ No  
(b) Acquisition of all rights, licenses, releases and consent for all content, products or services used or created by or for you. ☐ Yes ☐ No  
(c) Procedures to prevent the unauthorized disclosure or use of content, Information or material received in writing from the disclosing party pursuant to the terms and conditions of a Non-disclosure Agreement or Confidentiality Agreement. ☐ Yes ☐ No  
(d) Legal review of all new products, services, and content prior to release or dissemination. ☐ Yes ☐ No

- (e) Hold-harmless and indemnification clauses in your vendor or supplier written contracts or agreements, which inure to your benefit for a third-party supplied intellectual property (IP). ☐ Yes ☐ No
- (f) Hold-harmless and indemnification provided to third parties are limited to their use of the Applicant's licensed software, content or other protected materials in accordance with a written contract or agreement. ☐ Yes ☐ No
- (g) Agreements with new employees and "work-for-hire" contractors, which that include signed statements prohibiting the use of a previous employer's or customer's intellectual property, know-how or trade secrets. ☐ Yes ☐ No
- (h) Annual audit to ensure that intellectual property—management policies are followed. ☐ Yes ☐ No
- (i) Legal review of your domain name or product/service designs, names or logos with respect to intellectual property laws (including trademark or service mark). ☐ Yes ☐ No
2. When advertising or promoting your products or services, do you use music, animation or likenesses of famous individuals in your advertisements?  
If "Yes", have you secured the proper licenses or permission for use? ☐ Yes ☐ No
3. Do you use sweepstakes or games of chance in the promotion of your products or services?  
If "Yes", are you in compliance with the laws and regulations pertaining to them in all jurisdictions? ☐ Yes ☐ No
4. Are any products sold or distributed by or for you or any services you offer sold or advertised:  
(a) as being compatible with, alike or a clone of another company's product or service? ☐ Yes ☐ No  
(b) as superior to or comparable to the products or services of others? ☐ Yes ☐ No  
If yes to either a) or b), is legal review performed prior to the sale or dissemination of such products or services? ☐ Yes ☐ No
5. Are you an Internet service provider, application service provider or other similar technology service provider, or do you own and/or operate an interactive Web site including features such as a bulletin board, chat room or newsgroup?  
If "Yes", do you have a formalized notice and take-down procedure? ☐ Yes ☐ No
6. Do you have a formal Intellectual Property due-diligence process?  
If "Yes", does that process include the following. ☐ Yes ☐ No
- Identification of all IP assets involved with the sale ☐ Yes ☐ No
  - Certification of ownership title of all IP assets ☐ Yes ☐ No
  - Analysis of all legal opinions relating to IP assets ☐ Yes ☐ No
  - Review of any employment contracts pertaining to ownership of IP assets ☐ Yes ☐ No
  - An audit of the IP clearance procedures ☐ Yes ☐ No
7. Have you sold any companies during the past three years? ☐ Yes ☐ No  
If "Yes", do you have written contracts relating to any of the IP assets retained? ☐ Yes ☐ No
8. What percentage of your revenue is derived from products or services that are:
- Less than one year old \_\_\_\_\_%
  - Between one and two years old \_\_\_\_\_%
  - Between two and five years old \_\_\_\_\_%
  - Over five years old \_\_\_\_\_%
  - Upgrades of existing products \_\_\_\_\_%

9. Do you have a written process regarding securing the ownership or use rights of all applicable intellectual property, including source and object code? ☐ Yes ☐ No
- Does this include determining rights and duties pertaining to open source code? ☐ Yes ☐ No
  - With respect to securing such rights pertaining to source or object code, do you use a third party (e.g. software IP assessment firm)? ☐ Yes ☐ No
- If Yes, please provide the name of the third-party firm: \_\_\_\_\_
10. Do you receive hold-harmless or indemnification agreements from all third parties who supply source or object code? ☐ Yes ☐ No
- Does this policy include securing hold-harmless and indemnification agreements from third-party suppliers of source or object code? ☐ Yes ☐ No
11. Do you have written policies or procedures in place for auditing compliance with software licenses? ☐ Yes ☐ No

**V. INCIDENT AND LOSS HISTORY:**

1. Attach a complete description of the claims, suits and circumstances, including whether you reported such claims, suits or circumstances to an insurance carrier or sought indemnification from a third party. ☐ Yes ☐ No
2. In the past five (5) years, have any of **your** products been recalled (voluntary or mandated) from use? ☐ Yes ☐ No
- If "Yes", attach a complete description of the recall, including whether you reported the recall to any insurance carrier.
3. In the past five (5) years, have there been any administrative, civil or criminal investigations of **you** by any governmental or regulatory authority? ☐ Yes ☐ No
4. Have you been cited within the past three years for a regulatory violation? ☐ Yes ☐ No

**VI: APPLICANT ACKNOWLEDGEMENT**

**NOTICE TO APPLICANT - PLEASE READ CAREFULLY.**

INFORMATION OR DATA CONTAINED IN OR SUBMITTED IN CONNECTION WITH THIS APPLICATION (OR OTHERWISE TO ANY OF THE MEMBER INSURERS OF CHUBB GROUP OF INSURANCE COMPANIES ("CHUBB") IN CONNECTION WITH THE UNDERWRITING PROCESS) DOES NOT CONSTITUTE NOTICE OF AN OCCURRENCE, WRONGFUL ACT, CLAIM, SUIT OR OTHER CIRCUMSTANCE AND DOES NOT SATISFY ANY OF THE REPORTING NOTIFICATION OR OTHER PROVISIONS OF ANY POLICY. ALL SUCH NOTICES MUST BE GIVEN SEPARATELY IN ACCORDANCE WITH THE APPLICABLE POLICY CONDITIONS.

For the purposes of this application, the above-signed officer of all person(s) and entity(ies) proposed for this insurance declares and acknowledges by clicking where indicated below that he/she has reviewed this application and the statements contained therein with his/her Chief Executive Officer, Chief Financial Officer, Chief Operating Officer or their equivalents and that, to the best of their knowledge and belief, after reasonable inquiry, the statements in this application, and in any attachments, are true and complete. Chubb is authorized to make any inquiry in connection with this application. Signing this application shall not constitute a binder or obligate Chubb to complete this insurance, but it is agreed this application shall be the basis upon which a policy may be issued.

If the statements in this application or in any attachment change materially before the effective date of any proposed policy, the applicant must notify Chubb, and Chubb may modify or withdraw any quotation.

You understand that the limit of liability under any policy to be issued in response hereto shall include both indemnity payments for claims and payment of claim and defense expenses, as defined in the policy.

**PLEASE NOTE: ONLY DULY APPOINTED AGENTS OF CHUBB AND LICENSED BROKERS ARE AUTHORIZED TO SOLICIT APPLICATIONS FOR INSURANCE. AGENTS AND BROKERS ARE NOT AUTHORIZED TO BIND INSURANCE. NO INSURANCE SHALL BE PROVIDED UNLESS CHUBB ACCEPTS THE APPLICATION AND BINDS THE INSURANCE.**



By signing below, applicant hereby certifies that the statements made and the information and data supplied herewith are true, accurate and complete.

<u>Authorized Signature of Applicant</u>	<u>Date</u>	
<u>Print Name</u>	<u>Title</u>	
<b>Applicant</b>	<b>Authorized Agent (Please Print Name)</b>	
<b>Authorized Agent (Signature)</b>	<b>Title</b>	<b>Date</b>
<b>Submitted By (Insurance Agent)</b>	<b>Insurance Agency</b>	
<b>Agent License No. (For non-admitted placements a copy of valid surplus lines license will be required)</b>		
<b>Address (No., Street, City, State, and ZIP Code)</b>		

**NOTICE TO APPLICANT - PLEASE READ CAREFULLY.**

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, INCLUDING BUT NOT LIMITED TO FINES, DENIAL OF INSURANCE BENEFITS, CIVIL DAMAGES, CRIMINAL PROSECUTION AND CONFINEMENT IN STATE PRISON.

**APPLICABLE IN:**

**ARKANSAS**

ANY PERSON WHO KNOWINGLY PRESENTS 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.

**COLORADO**

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.

**DISTRICT OF COLUMBIA**

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.

**FLORIDA**

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.

**KENTUCKY**

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.

---

**LOUISIANA**

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.

**MAINE**

IT IS A CRIME TO KNOWINGLY PROVIDE FALSE, INCOMPLETE OR MISLEADING INFORMATION TO INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES OR A DENIAL OF INSURANCE BENEFITS.

**MARYLAND**

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

**NEW JERSEY**

ANY PERSON WHO INCLUDES ANY FALSE OR MISLEADING INFORMATION ON AN APPLICATION FOR AN INSURANCE POLICY IS SUBJECT TO CRIMINAL AND CIVIL PENALTIES.

**NEW MEXICO**

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.

**NEW YORK**

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.

**OHIO**

ANY PERSON WHO, WITH THE 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.

**OKLAHOMA**

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.

**OREGON**

ANY PERSON, WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON, FILES AN APPLICATION FOR INSURANCE CONTAINING ANY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING INFORMATION CONCERNING ANY MATERIAL FACT THERETO, MAY BE GUILTY OF AN INSURANCE FRAUD.

**PENNSYLVANIA**

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.

**TENNESSEE, VIRGINIA AND WASHINGTON**

IT IS A CRIME TO KNOWINGLY PROVIDE FALSE, INCOMPLETE OR MISLEADING INFORMATION TO INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING THE COMPANY. PENALTIES INCLUDE IMPRISONMENT, FINES AND DENIAL OF INSURANCE BENEFITS.

**RHODE ISLAND AND WEST VIRGINIA**

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.

This application is protected by copyright laws and should not be reproduced or redistributed without the express written consent of Chubb, A Division of Federal Insurance Company. All rights reserved.

## Chubb Cyber Enterprise Risk Management Policy

## Cyber and Privacy Insurance

New Business Application

This is a static sample document for demonstration / discussion purposes only. This not intended to represent a current version of an application; please do not use it for actual form submittal.

## NOTICE

**NOTICE: THE THIRD PARTY LIABILITY INSURING AGREEMENTS OF THIS POLICY PROVIDE CLAIMS-MADE COVERAGE, WHICH APPLIES ONLY TO CLAIMS FIRST MADE DURING THE POLICY PERIOD OR AN APPLICABLE EXTENDED REPORTING PERIOD FOR ANY INCIDENT TAKING PLACE AFTER THE RETROACTIVE DATE BUT BEFORE THE END OF THE POLICY PERIOD.**

AMOUNTS INCURRED AS CLAIMS EXPENSES UNDER THIS POLICY SHALL REDUCE AND MAY EXHAUST THE APPLICABLE LIMIT OF INSURANCE AND WILL BE APPLIED AGAINST ANY APPLICABLE RETENTION. IN NO EVENT WILL THE INSURER BE LIABLE FOR CLAIMS EXPENSES OR THE AMOUNT OF ANY JUDGMENT OR SETTLEMENT IN EXCESS OF THE APPLICABLE LIMIT OF INSURANCE. TERMS THAT ARE UNDERLINED IN THIS NOTICE PROVISION HAVE SPECIAL MEANING AND ARE DEFINED IN SECTION II, DEFINITIONS. READ THE ENTIRE POLICY CAREFULLY.

## INSTRUCTIONS

Please respond to answers clearly. Underwriters will rely on all statements made in this **Application**. This form must be dated and signed.

## 1. Applicant Information

**Desired Effective Date**

Mm/dd/yyyy

**Applicant Name**

Click here to enter text.

**Applicant Address (City, State, Zip)**

Click here to enter text.

**Please list all Subsidiaries for which coverage is desired:**

Click here to enter text.

**Applicant Type**

Choose an item.

**Ownership Structure**

Choose an item.

**Website Address**

Click here to enter text.

**Year Established**

Click here to enter text.

**Global Revenue (Prior Fiscal Year)**

Click here to enter text.

**% Domestic Revenue**

Click here to enter text.

**Global Revenue (Current Projected Fiscal Year)**

Click here to enter text.

**% Online Revenue**

Click here to enter text.

**Total Number of Employees**

Enter a number or choose an item.

## Chubb Cyber Enterprise Risk Management Policy

---

**Number of Records Containing Protected Information:**

What is the maximum total number of unique individual persons or organizations whose **Protected Information** could be compromised in a not-yet-discovered **Cyber Incident**, or will be stored or transmitted during the **Policy Period** on the Applicant's **Computer System** or any **Shared Computer System** combined that relate to the Applicant's business?

This should include **Protected Information** of employees, retirees, customers, partners and other third parties that the Applicant is responsible for securing, including **Protected Information** that is secured by third parties under contract with the Applicant. Multiple records or types of **Protected Information** relating to the same unique individual person or organization should be considered a single record.

Enter a number or choose an item

---

**2. Nature of Operations****Class of Business**

Describe nature of business operations, products or services in layperson terms.

Does the Applicant currently or will the Applicant potentially operate as any of the following?

- |                                    |   |
|------------------------------------|---|
| • Accreditation Services Provider  | • Manufacturer of Life Safety Products/Software |
| • Adult Content Provider           | • Media Production Company                      |
| • Credit Bureau                    | • Payment Processor                             |
| • Cryptocurrency Exchange          | • Peer To Peer File Sharing                     |
| • Data Aggregator/Broker/Warehouse | • Social Media                                  |
| • Direct Marketer                  | • Surveillance                                  |
| • Gambling Services Provider       | • Third Party Claims Administrator              |

Or does the Applicant derive more than 50% of its revenue from technology products and services (e.g. software, electronics, telecom)?

☐ Yes ☐ No

**If Yes**, please provide details:

[Click here to enter text.](#)

---

**3. Current Loss Information**

Within the past three years, has the Applicant had any actual or potential **Incidents** or **Claims** to which the **Policy** would apply; or is the Applicant aware of any fact, circumstance, or situation that could reasonably be expected to give rise to an **Incident** or **Claim** to which the **Policy** would apply? ☐ Yes ☐ No

**If Yes** please provide details:

[Click here to enter text.](#)

---

## Chubb Cyber Enterprise Risk Management Policy

## 4. Cyber and Media Controls

Which of the following IT security controls does the Applicant have in place?

- |  |   |
|--|---|
| 1) Antivirus and Firewalls (Windows 7 or higher qualifies) | <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown |
| 2) Encryption of Sensitive Data                            | <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown |
| 3) Encryption of Mobile Computing Devices                  | <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown |
| 4) Critical Software Patching Procedures                   | <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown |
| 5) Critical Data Backup and Recovery Procedures            | <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown |
| 6) Formal Cyber Incident Response Plan                     | <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown |

Does the Applicant accept payment card (Credit/debit card) transactions?

☐ Yes ☐ No**If Yes**, is the Applicant PCI compliant? (via assessment or self-attestation)☐ Yes ☐ No ☐ Unknown

Does the Applicant deal with protected health information as defined by HIPAA?

☐ Yes ☐ No**If Yes**, is Applicant compliant with HIPAA and the HITECH Act?☐ Yes ☐ No ☐ Unknown

Does the Applicant have operations or customers in California, or any responsibilities under the California Confidentiality of Medical Information Act?

☐ Yes ☐ No ☐ Unknown

Has the Applicant obtained legal review of its use of trademarks, including domain names?

☐ Yes ☐ No ☐ Unknown

## 5. Current Coverage

Does the Applicant currently purchase Professional Liability or E&amp;O insurance?

☐ Yes ☐ No**If Yes**, what is the Retro Date? [Click here to enter a date.](#)

Does the Applicant currently purchase Cyber or Privacy Liability insurance?

☐ Yes ☐ No**If Yes**, what is the Retro Date? [Click here to enter a date.](#)

Does the Applicant currently purchase Media Liability Insurance?

☐ Yes ☐ No**If Yes**, what is the Retro Date? [Click here to enter a date.](#)

Does the Applicant intend to purchase E&amp;O and/or Media coverage on a separate and distinct policy? (e.g. with a separate set of limits, or with another carrier?)

☐ Yes ☐ No

## 6. Desired Coverage (Only Enter Information For Desired Coverages)

	Retention	Limit	Commentary
--	-----------	-------	------------

Cyber and Media Coverages

\$

\$

Enter any further commentary about desired coverage options.

[Click here to enter text.](#)

## FRAUD WARNING STATEMENTS

---

The Applicant's submission of this **Application** does not obligate the **Insurer** to issue, or the Applicant to purchase, a policy. The Applicant will be advised if the **Application** for coverage is accepted. The Applicant hereby authorizes the **Insurer** to make any inquiry in connection with this **Application**.

**Notice to Arkansas, Minnesota, New Mexico and Ohio Applicants:** Any person who, with intent to defraud or knowing that he/she is facilitating a fraud against an insurer, submits an application or files a claim containing a false, fraudulent or deceptive statement is, or may be found to be, guilty of insurance fraud, which is a crime, and may be subject to civil fines and criminal penalties.

**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 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.

**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 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 and Rhode Island 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, 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.

**Notice to Alabama and 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 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 and Texas Applicants:** Any person who makes an intentional misstatement that is material to the risk may be found guilty of insurance fraud by a court of law.

**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 Puerto Rico Applicants:** Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation with the penalty of a fine of not less than five thousand (5,000) dollars and not more than ten thousand (10,000) dollars, or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances are present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

**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, 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.

## MATERIAL CHANGE

---

If there is any material change in the answers to the questions in this **Application** before the **Policy** inception date, the Applicant must immediately notify the **Insurer** in writing, and any outstanding quotation may be modified or withdrawn.

## DECLARATION AND SIGNATURE

---

For the purposes of this **Application**, the undersigned authorized agents of the person(s) and entity(ies) proposed for this insurance declare to the best of their knowledge and belief, after reasonable inquiry, the statements made in this **Application** and any attachments or information submitted with this **Application**, are true and complete. The undersigned agree that this **Application** and its attachments shall be the basis of a contract should a policy providing the requested coverage be issued and shall be deemed to be attached to and shall form a part of any such policy. The **Insurer** will have relied upon this **Application**, its attachments, and such other information submitted therewith in issuing any policy.

The information requested in this **Application** is for underwriting purposes only and does not constitute notice to the **Insurer** under any policy of a Claim or potential Claim.

This **Application** must be signed by the risk manager or a senior officer of the **Named Insured**, acting as the authorized representative of the person(s) and entity(ies) proposed for this insurance.

Date

Signature

Title

---

**SIGNATURE - FOR ARKANSAS, MISSOURI, NEW MEXICO, NORTH DAKOTA AND WYOMING APPLICANTS ONLY**

---

PLEASE ACKNOWLEDGE AND SIGN THE FOLLOWING DISCLOSURE TO YOUR **APPLICATION** FOR INSURANCE:

I UNDERSTAND AND ACKNOWLEDGE THAT THE **POLICY** FOR WHICH I AM APPLYING CONTAINS A DEFENSE WITHIN LIMITS PROVISION WHICH MEANS THAT **CLAIMS EXPENSES** WILL REDUCE MY LIMITS OF INSURANCE AND MAY EXHAUST THEM COMPLETELY. SHOULD THAT OCCUR, I SHALL BE LIABLE FOR ANY FURTHER CLAIMS **EXPENSES** AND **DAMAGES**.

Applicant's Signature (Arkansas, Missouri, New Mexico, North Dakota & Wyoming Applicants, In Addition To **Application** Signature Above):

Signed: \_\_\_\_\_ (must be Officer of Applicant)

Print Name & Title: \_\_\_\_\_

Date (MM/DD/YY): \_\_\_\_\_

Email/Phone: \_\_\_\_\_

**SIGNATURE - FOR KANSAS AND ALASKA APPLICANTS ONLY**

---

ELECTRONIC DELIVERY SUPPLEMENT:

You are required by law to obtain consent from insureds prior to engaging in any electronic delivery of insurance policies and/or other supporting documents in connection with the **Policy**. You have the right to:

Select electronic delivery - check here \_\_\_\_\_

Reject electronic delivery – check here \_\_\_\_\_

Applicant's Signature (Kansas and Alaska Applicants, In Addition To **Application** Signature Above):

**FOR FLORIDA APPLICANTS ONLY:**

---

Agent Name: \_\_\_\_\_

Agent License ID Number: \_\_\_\_\_

**FOR IOWA APPLICANTS ONLY:**

---

Broker: \_\_\_\_\_

Address: \_\_\_\_\_



This is a static sample document for demonstration / discussion purposes only. This not intended to represent a current version of an application; please do not use it for actual form submittal.

## Travelers Casualty and Surety Company of America

## CyberRisk Short Form Application

**Claims-Made:** The information requested in this Application is for a Claims-Made policy. If issued, the policy will apply only to claims first made during the policy period, or any applicable extended reporting period.

**Defense Within Limits:** The limit of liability available to pay losses will be reduced and may be completely exhausted by amounts paid as defense costs.

### IMPORTANT INSTRUCTIONS

This Application will only be accepted for Applicants with revenues of \$50,000,000 or less **and** assets of \$500,000,000 or less.

Under this CyberRisk Coverage, affiliates, other than Subsidiaries as defined in this coverage, are not covered unless the Insurer has agreed specifically to schedule such entities by endorsement.

### GENERAL INFORMATION

Name of Applicant:

Street Address:

City: State: Zip:

Applicant website: Year Established: NAICS Code:

Total assets as of most recent fiscal year-end: \$ Annual revenues as of most recent fiscal year-end: \$

Entity type (select all that apply):

☐ Private ☐ Nonprofit ☐ Financial Institution ☐ Publicly Traded ☐ Franchisor or Franchisee ☐ Homeowner or Condo Association

### UNDERWRITING INFORMATION

1. Indicate whether the Applicant has:
  - a. Up-to-date, active firewall technology ☐ Yes ☐ No
  - b. Up-to-date, active anti-virus software on all computers, networks, and mobile devices ☐ Yes ☐ No
  - c. A process in place to regularly download and install patches ☐ Yes ☐ No
  - d. Backup and recovery procedures in place for all important business and customer data ☐ Yes ☐ No
  - e. An incident response plan to respond to a network intrusion ☐ Yes ☐ No
  - f. A disaster recovery plan, business continuity plan, or equivalent to respond to a computer system disruption ☐ Yes ☐ No
  - g. Controls to ensure the content of media communications and websites are lawful ☐ Yes ☐ No
  - h. Procedures in place which require service providers with access to the Applicant's systems or the Applicant's confidential information to demonstrate adequate network security controls ☐ Yes ☐ No
  - i. Multi-factor authentication for remote access to email and other systems and programs that contain private or sensitive data in bulk ☐ Yes ☐ No ☐ N/A
2. Is the Applicant currently compliant with Payment Card Industry Data Security Standards (PCI-DSS)? ☐ Yes ☐ No ☐ N/A
3. Is the Applicant HIPAA compliant? ☐ Yes ☐ No ☐ N/A
4. Indicate whether the Applicant encrypts private or sensitive data:
  - a. While at rest in the Applicant's database or on the Applicant's network ☐ Yes ☐ No ☐ N/A
  - b. While in transit in electronic form ☐ Yes ☐ No ☐ N/A
  - c. While on mobile devices ☐ Yes ☐ No ☐ N/A
  - d. While on employee owned devices ☐ Yes ☐ No ☐ N/A
  - e. While in the care, custody, and control of a third party service provider ☐ Yes ☐ No ☐ N/A

## LOSS INFORMATION

---

5. In the past three years, has the Applicant:
- a. Experienced: (1) a network or computer system disruption due to an intentional attack or system failure; (2) an actual or suspected data breach; or (3) a cyber extortion demand? ☐ Yes ☐ No
  - b. Received any complaints, claims, or been subject to any litigation involving:  
Matters of data protection law, intellectual property rights, defamation, rights of privacy, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks, or access to the Applicant's network? ☐ Yes ☐ No
6. Is the Applicant, any Subsidiary, or any person proposed for this insurance aware of any circumstance that could give rise to a claim against them under this CyberRisk coverage? ☐ Yes ☐ No

*If the Applicant answered Yes to any part of Question 5 or Question 6, attach details of each claim, complaint, allegation, or incident, including costs, losses, or damages incurred or paid, any corrective procedures to avoid such allegations in the future, and any amounts paid as loss under any insurance policy.*

## REQUESTED INSURANCE TERMS

---

7. Requested Terms:
- Aggregate Limit Requested: \$ \_\_\_\_\_
- Retention Requested: \$ \_\_\_\_\_
- Effective Date Requested: \_\_\_\_\_
8. Does the Applicant currently purchase CyberRisk coverage? ☐ Yes ☐ No
- If Yes, provide the following:*
- Expiring Carrier: \_\_\_\_\_
- Expiring Limit: \$ \_\_\_\_\_
- Date coverage first purchased? \_\_\_\_\_

## ORGANIZATIONS NOT ELIGIBLE FOR COVERAGE

---

Coverage will not be considered for companies involved in whole or in part with paramilitary operations, pornography, adult entertainment, escort services, prostitution, or the manufacturing, distribution, or sale of marijuana.

## NOTICE REGARDING COMPENSATION

---

For information about how Travelers compensates independent agents, brokers, or other insurance producers, please visit this website: [http://www.travelers.com/w3c/legal/Producer\\_Compensation\\_Disclosure.html](http://www.travelers.com/w3c/legal/Producer_Compensation_Disclosure.html)

If you prefer, you can call the following toll-free number: 1-866-904-8348. Or you can write to us at Travelers, Agency Compensation, One Tower Square, Hartford, CT 06183.

## FRAUD STATEMENTS – ATTENTION APPLICANTS IN THE FOLLOWING JURISDICTIONS

---

**ALABAMA, ARKANSAS, DISTRICT OF COLUMBIA, MARYLAND, NEW MEXICO, AND RHODE ISLAND:** Any person who knowingly (or willfully in MD) presents a false or fraudulent claim for payment of a loss or benefit or who knowingly (or willfully in MD) presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

**COLORADO:** It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company to defraud or attempt 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 to defraud or attempt to defraud the policyholder or claimant regarding a settlement or award payable from insurance proceeds will be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

**FLORIDA:** 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.

**KENTUCKY, NEW JERSEY, NEW YORK, OHIO, AND PENNSYLVANIA:** 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. (In New York, the civil penalty is not to exceed five thousand dollars (\$5,000) and the stated value of the claim for each such violation.)

**LOUISIANA, MAINE, TENNESSEE, VIRGINIA, AND WASHINGTON:** It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company to defraud the company. Penalties include imprisonment, fines, and denial of insurance benefits.

**OREGON:** 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 may be guilty of a crime and may be subject to fines and confinement in prison.

**PUERTO RICO:** Any person who knowingly and intending to defraud presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, will incur a felony and, upon conviction, will be sanctioned for each violation with the penalty of a fine of not less than \$5,000 and not over \$10,000, or a fixed term of imprisonment for three years, or both penalties. Should aggravating circumstances be present, the penalty established may be increased to a maximum of five years; if extenuating circumstances are present, it may be reduced to a minimum of two years.

## ***SIGNATURES***

The undersigned Authorized Representative represents that to the best of his or her knowledge and belief, and after reasonable inquiry, the statements provided in response to this Application are true and complete, and, except in NC, may be relied upon by Travelers as the basis for providing insurance. The Applicant will notify Travelers of any material changes to the information provided.

☐ Electronic Signature and Acceptance – Authorized Representative\*

\*If electronically submitting this document, electronically sign this form by checking the Electronic Signature and Acceptance box above. By doing so, the Applicant agrees that use of a key pad, mouse, or other device to check the Electronic Signature and Acceptance box constitutes acceptance and agreement as if signed in writing and has the same force and effect as a signature affixed by hand.

Authorized Representative Signature: <b>X</b>	Authorized Representative Name, Title, and email address:	Date ( <i>month/dd/yyyy</i> ):
Producer Name (required in FL & IA): <b>X</b>	State Producer License No (required in FL):	Date ( <i>month/dd/yyyy</i> ):
Agency:	Agency contact and email address:	Agency Phone Number:

## ***ADDITIONAL INFORMATION***



This is a static sample document for demonstration / discussion purposes only. This not intended to represent a current version of an application; please do not use it for actual form submittal.

## Travelers Casualty and Surety Company of America

## CyberRisk Application

**Claims-Made:** The information requested in this Application is for a Claims-Made policy. If issued, the policy will apply only to claims first made during the policy period, or any applicable extended reporting period.

**Defense Within Limits:** The limit of liability available to pay losses will be reduced and may be completely exhausted by amounts paid as defense costs.

### IMPORTANT INSTRUCTIONS

Under this CyberRisk Coverage, affiliates, other than Subsidiaries as defined in this coverage, are not covered unless the Insurer has agreed specifically to schedule such entities by endorsement.

### GENERAL INFORMATION

Name of Applicant:

Street Address:

City: State: Zip:

Applicant website: Year Established: NAICS Code:

Total assets as of most recent fiscal year-end: Annual revenues as of most recent fiscal year-end:  
\$ \$

Entity type (select all that apply):

☐ Private ☐ Nonprofit ☐ Financial Institution ☐ Publicly Traded ☐ Franchisor or Franchisee ☐ Homeowner or Condo Association

### UNDERWRITING INFORMATION

#### DATA INVENTORY

1. Indicate whether the Applicant or a third party on the Applicant's behalf, collects, receives, processes, transmits, or maintains the following types of data as part of its business activities:

a. Credit/Debit Card Data ☐ Yes ☐ No

If Yes:

i. Is the Applicant currently compliant with Payment Card Industry Data Security Standards (PCI-DSS)? ☐ Yes ☐ No

ii. How many credit card transactions are processed or accepted for payment in a typical year?

iii. What is the Applicant's reporting level? ☐ 1 ☐ 2 ☐ 3 ☐ 4

iv. Was the Applicant's last PCI assessment conducted within the past 12 months? ☐ Yes ☐ No

b. Medical information, other than that of the Applicant's own employees ☐ Yes ☐ No

c. Non-employee Social Security Numbers ☐ Yes ☐ No

d. Employee/HR Information ☐ Yes ☐ No

2. What is the approximate number of unique individuals for whom the Applicant, or a third party on the Applicant's behalf, collects, stores, or processes any amount of personal information as outlined in Question 1?

☐ fewer than 100,000 ☐ 100,000 – 250,000 ☐ 250,001 – 500,000 ☐ 500,001 – 1,000,000

☐ 1,000,001 – 2,500,000 ☐ 2,500,001 – 5,000,000 ☐ > 5,000,000

3. Indicate whether the data indicated in Question 1 is encrypted:

a. While at rest in the Applicant's databases or on the Applicant's network ☐ Yes ☐ No ☐ N/A

b. While in transit in electronic form ☐ Yes ☐ No ☐ N/A

c. While on mobile devices ☐ Yes ☐ No ☐ N/A

- d. While on employee owned devices ☐ Yes ☐ No ☐ N/A
- e. While in the care, custody, and control of a third party service provider ☐ Yes ☐ No ☐ N/A
4. Is the Applicant a Healthcare Provider, Business Associate, or Covered Entity under HIPAA?  
*If Yes, is the Applicant HIPAA compliant?* ☐ Yes ☐ No  
☐ Yes ☐ No
5. Is the Applicant subject to the General Data Protection Regulation (GDPR)?  
*If Yes, is the Applicant currently compliant with GDPR?* ☐ Yes ☐ No  
*If the Applicant is subject to GDPR, and is not currently compliant, attach a description of steps being taken toward compliance.* ☐ Yes ☐ No

#### PRIVACY CONTROLS

6. Indicate whether the Applicant currently has the following in place:
- a. A Chief Privacy Officer or other individual assigned responsibility for monitoring changes in statutes and regulations related to handling and use of sensitive information ☐ Yes ☐ No
  - b. A publicly available privacy policy which has been reviewed by an attorney ☐ Yes ☐ No
  - c. Sensitive data classification and inventory procedures ☐ Yes ☐ No
  - d. Data retention, destruction, and recordkeeping procedures ☐ Yes ☐ No
  - e. Annual privacy and information security training for employees ☐ Yes ☐ No
  - f. Restricted access to sensitive data and systems based on job function ☐ Yes ☐ No

#### NETWORK SECURITY CONTROLS

7. Indicate whether the Applicant currently has the following in place:
- a. A Chief Information Security Officer or other individual assigned responsibility for privacy and security practices ☐ Yes ☐ No
  - b. Up-to-date, active firewall technology ☐ Yes ☐ No
  - c. Up-to-date, active anti-virus software on all computers, networks, and mobile devices ☐ Yes ☐ No
  - d. A process in place to regularly download, test, and install patches  
*If Yes, is this process automated?* ☐ Yes ☐ No  
*If Yes, are critical patches installed within 30 days of release?* ☐ Yes ☐ No
  - e. Intrusion Detection System (IDS) ☐ Yes ☐ No
  - f. Intrusion Prevention System (IPS) ☐ Yes ☐ No
  - g. Data Loss Prevention System (DLP) ☐ Yes ☐ No
  - h. Multi-factor authentication for administrative or privileged access ☐ Yes ☐ No ☐ N/A
  - i. Multi-factor authentication for remote access to the Applicant's network and other systems and programs that contain private or sensitive data in bulk ☐ Yes ☐ No ☐ N/A
  - j. Multi-factor authentication for remote access to email ☐ Yes ☐ No ☐ N/A
  - k. Remote access to the Applicant's network limited to VPN ☐ Yes ☐ No ☐ N/A
  - l. Backup and recovery procedures in place for all important business and customer data  
*If Yes, are such procedures automated?* ☐ Yes ☐ No  
*If Yes, are such procedures tested on an annual basis?* ☐ Yes ☐ No
  - m. Annual penetration testing  
*If Yes, is such testing conducted by a third party service provider?* ☐ Yes ☐ No
  - n. Annual network security assessments  
*If Yes, are such assessments conducted by a third party service provider?* ☐ Yes ☐ No
  - o. Systematic storage and monitoring of network and security logs ☐ Yes ☐ No
  - p. Enforced password complexity requirements ☐ Yes ☐ No
  - q. Procedures in place to terminate user access rights as part of the employee exit process ☐ Yes ☐ No

#### PAYMENT CARD CONTROLS

Complete only if the Applicant, or a third party on the Applicant's behalf, collects, processes, stores, or accepts payment card information.

8. Indicate whether the Applicant's current payment card environment:
- a. Processes all payment cards using End-to-End or Point-to-Point encryption ☐ Yes ☐ No
  - b. Encrypts or tokenizes card data when stored ☐ Yes ☐ No
  - c. Processes card present transactions using EMV capable devices ☐ Yes ☐ No ☐ N/A



## CONTENT LIABILITY CONTROLS

☐ Communications And Media Liability Coverage is not requested.

9. Does the Applicant have a comprehensive written program in place for managing intellectual property rights? ☐ Yes ☐ No
10. Indicate whether the Applicant has formal policies or procedures for:
- a. Avoiding the dissemination of content that infringes upon intellectual property rights ☐ Yes ☐ No
  - b. Editing or removing controversial, offensive, or infringing content from material distributed or published by or on behalf of the Applicant ☐ Yes ☐ No
  - c. Responding to allegations that content created, displayed, or published by the Applicant is libelous, infringing upon, or in violation of a third party's privacy rights ☐ Yes ☐ No

## BUSINESS CONTINUITY / DISASTER RECOVERY / INCIDENT RESPONSE

11. Indicate whether the Applicant has the following:
- a. A disaster recovery plan, business continuity plan, or equivalent to respond to a computer system disruption ☐ Yes ☐ No
  - b. An incident response plan to respond to a network intrusion ☐ Yes ☐ No
12. Are all plans indicated above tested regularly with any critical deficiencies remediated? ☐ Yes ☐ No ☐ N/A
13. Based upon testing results, how long does it take to restore the Applicant's critical business operations following a network or systems interruption?
- ☐ Unknown ☐ 0 – 12 hours ☐ 12 – 24 hours ☐ More than 24 hours

## VENDOR CONTROLS

14. For vendors with access to the Applicant's computer system or confidential information, indicate whether the Applicant has the following in place:
- a. Written policies which specify appropriate vendor information security controls ☐ Yes ☐ No
  - b. Periodic review of, and updates to, vendor access rights ☐ Yes ☐ No
  - c. Prompt revocation of vendor access rights when access is no longer needed ☐ Yes ☐ No
  - d. Logging and monitoring of vendor access to the Applicant's system ☐ Yes ☐ No
  - e. A requirement that vendors carry their own Professional Liability or Cyber Liability insurance ☐ Yes ☐ No
  - f. Hold harmless / indemnity clauses that benefit the Applicant in contracts with vendors ☐ Yes ☐ No

15. Indicate which of the following services are outsourced:

Data back up <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Provider: _____	Payment processing <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Provider: _____
Data center hosting <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Provider: _____	Physical security <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Provider: _____
IT infrastructure <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Provider: _____	Software development <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Provider: _____
IT security <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Provider: _____	Customer marketing <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Provider: _____
Web hosting <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Provider: _____	Data processing <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Provider: _____

*If Data center hosting or IT infrastructure is answered Yes above:*

- a. What is the likely impact to the organization if these services become unavailable?

- b. Does the Applicant have an alternative solution in the event of a failure or outage to one of these service providers?

*If Payment processing is answered Yes above, does the Applicant have an alternative means of processing card data in the event of an outsourced provider failure or outage?*

☐ Yes ☐ No

*Provide details:* \_\_\_\_\_

## LOSS INFORMATION

16. In the past three years, has the Applicant experienced a network or computer system disruption due to an intentional attack or system failure; an actual or suspected data breach; an actual or attempted extortion demand; or received any complaints, claims, or been subject to litigation involving matters or privacy injury, identity theft, denial-of-service attacks, computer virus infections, theft of information, damage to third party networks, or the Applicant's customer's ability to rely on the Applicant's network? ☐ Yes ☐ No

17. Is the Applicant, any Subsidiary, or any person proposed for this insurance aware of any circumstance that could give rise to a claim against them under this CyberRisk Coverage? ☐ Yes ☐ No

*If the Applicant answered Yes to any part of Question 16 or Question 17, attach details of each claim, complaint, allegation, or incident, including costs, losses, or damages incurred or paid, any corrective procedures to avoid such allegations in the future, and any amounts paid as loss under any insurance policy.*

## REQUESTED INSURANCE TERMS

Requested Terms:

Insuring Agreement	Limit Requested	Retention Requested
Privacy And Security	\$	\$
Media	\$	\$
Regulatory Proceedings	\$	\$
Privacy Breach Notification	\$	\$
Computer And Legal Experts	\$	\$
Betterment	\$	\$
Cyber Extortion	\$	\$
Data Restoration	\$	\$
Public Relations	\$	\$
Computer Fraud	\$	\$
Funds Transfer Fraud	\$	\$
Social Engineering Fraud	\$	\$
Telecom Fraud	\$	\$
Business Interruption	\$	\$
Dependent Business Interruption	\$	\$
Reputation Harm	\$	\$

18. Requested Terms:  
Aggregate Limit Requested: \$  
Effective Date Requested:

19. Does the Applicant currently purchase CyberRisk coverage? ☐ Yes ☐ No

*If Yes, provide the following:*

Expiring Carrier:  
Expiring Limit: \$  
Date coverage first purchased?

## REQUIRED ATTACHMENTS

As part of this Application, provide copies of the documents listed below. Such documents are made a part of this Application; the Insurer may elect to obtain requested information from public sources, including the Internet.

- CyberRisk Employed Lawyers Supplement to be completed if Employed Lawyers coverage is sought.

## ORGANIZATIONS NOT ELIGIBLE FOR COVERAGE

Coverage will not be considered for companies involved in whole or in part with paramilitary operations, pornography, adult entertainment, escort services, prostitution, or the manufacturing, distribution, or sale of marijuana.

## NOTICE REGARDING COMPENSATION

For information about how Travelers compensates independent agents, brokers, or other insurance producers, please visit this website: [http://www.travelers.com/w3c/legal/Producer\\_Compensation\\_Disclosure.html](http://www.travelers.com/w3c/legal/Producer_Compensation_Disclosure.html)

If you prefer, you can call the following toll-free number: 1-866-904-8348. Or you can write to us at Travelers, Agency Compensation, One Tower Square, Hartford, CT 06183.

## FRAUD STATEMENTS – ATTENTION APPLICANTS IN THE FOLLOWING JURISDICTIONS

**ALABAMA, ARKANSAS, DISTRICT OF COLUMBIA, MARYLAND, NEW MEXICO, AND RHODE ISLAND:** Any person who knowingly (or willfully in MD) presents a false or fraudulent claim for payment of a loss or benefit or who knowingly (or willfully in MD) presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

**COLORADO:** It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company to defraud or attempt 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 to defraud or attempt to defraud the policyholder or claimant regarding a settlement or award payable from insurance proceeds will be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

**FLORIDA:** 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.

**KENTUCKY, NEW JERSEY, NEW YORK, OHIO, AND PENNSYLVANIA:** 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. (In New York, the civil penalty is not to exceed five thousand dollars (\$5,000) and the stated value of the claim for each such violation.)

**LOUISIANA, MAINE, TENNESSEE, VIRGINIA, AND WASHINGTON:** It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company to defraud the company. Penalties include imprisonment, fines, and denial of insurance benefits.

**OREGON:** 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 may be guilty of a crime and may be subject to fines and confinement in prison.

**PUERTO RICO:** Any person who knowingly and intending to defraud presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, will incur a felony and, upon conviction, will be sanctioned for each violation with the penalty of a fine of not less than \$5,000 and not over \$10,000, or a fixed term of imprisonment for three years, or both penalties. Should aggravating circumstances be present, the penalty established may be increased to a maximum of five years; if extenuating circumstances are present, it may be reduced to a minimum of two years.

## SIGNATURES

The undersigned Authorized Representative represents that to the best of his or her knowledge and belief, and after reasonable inquiry, the statements provided in response to this Application are true and complete, and, except in NC, may be relied upon by Travelers as the basis for providing insurance. The Applicant will notify Travelers of any material changes to the information provided.

☐ Electronic Signature and Acceptance – Authorized Representative\*

\*If electronically submitting this document, electronically sign this form by checking the Electronic Signature and Acceptance box above. By doing so, the Applicant agrees that use of a key pad, mouse, or other device to check the Electronic Signature and Acceptance box constitutes acceptance and agreement as if signed in writing and has the same force and effect as a signature affixed by hand.

Authorized Representative Signature: <b>X</b>	Authorized Representative Name, Title, and email address:	Date (month/dd/yyyy):
Producer Name (required in FL & IA): <b>X</b>	State Producer License No (required in FL):	Date (month/dd/yyyy):
Agency:	Agency contact and email address:	Agency Phone Number:

## ADDITIONAL INFORMATION



## CyberRisk Social Engineering Fraud Supplement

### Travelers Casualty and Surety Company of America

**Claims-Made:** The information requested in this Application is for a Claims-Made policy. If issued, the policy will apply only to claims first made during the policy period, or any applicable extended reporting period.

**Defense Within Limits:** The limit of liability available to pay losses will be reduced and may be exhausted by amounts paid as defense costs.

### IMPORTANT INSTRUCTIONS

Under this CyberRisk Coverage, affiliates, other than Subsidiaries as defined in this coverage, are not covered unless the Insurer has agreed specifically to schedule such entities by endorsement.

### GENERAL INFORMATION

Applicant Name:

Street Address:

City:

State:

Zip:

### DESCRIPTION OF OPERATIONS

1. Does the Applicant make payments to third parties via a wire transfer system? ☐ Yes ☐ No  
*If Yes, how frequently are such payments made?* \_\_\_\_\_
2. Are all employees who are responsible for authorizing and executing payments or funds transfer requests provided anti-fraud training, including social engineering, phishing, masquerading, and other fraud schemes? ☐ Yes ☐ No

### VENDOR CONTROLS

3. Does the Applicant verify the authenticity of all vendor bank accounts by a direct call to the payment-receiving bank prior to the first time setup of such banking information in the Applicant's accounts payable system? ☐ Yes ☐ No
4. Does the Applicant have procedures in place to verify the authenticity of invoices and other payment requests received from a vendor? ☐ Yes ☐ No
5. Does the Applicant have procedures in place to verify the receipt of inventory, supplies, goods, or services against an invoice prior to making payment to a vendor? ☐ Yes ☐ No
6. Does the Applicant confirm all change requests regarding vendor account information (including all bank account information, invoice changes, telephone or Telefacsimile numbers, location, and contact information) by a direct call to the vendor using only the telephone number provided by the vendor before the change request was received? ☐ Yes ☐ No  
*If Yes:*
  - a. Is the call back procedure performed by an individual other than the individual who received the change request? ☐ Yes ☐ No
  - b. Does the Applicant refrain from implementing any such change requests until after the vendor has responded to the Applicant's inquiry regarding change request authenticity? ☐ Yes ☐ No
  - c. Does the Applicant confirm all such change requests made by a vendor with an individual (at the vendor) other than the individual who requested the change? ☐ Yes ☐ No
  - d. Does the Applicant require that all such change requests made by a vendor be approved by the Applicant's supervisor of the individual who received the change request, before it is acted upon? ☐ Yes ☐ No

7. Does the Applicant verify the length of time the account receiving the payment or funds transfer (e.g., wire transfer, ACH transfer, etc.) has been in existence with the receiving bank prior to approving and initiating any such transfer when it involves a recent change request? (e.g., any recent changes in depositing bank, bank routing number, or account number, etc.)? ☐ Yes ☐ No

### CLIENT CONTROLS

---

8. Does the Applicant have procedures (e.g. credit/background checks, physical location information, bank account information) in place to verify the authenticity of all clients? ☐ Yes ☐ No  
*If Yes:*  
a. Describe the procedures: \_\_\_\_\_  
b. Are such procedures applicable for each and every transaction prior to furnishing goods or services to clients? ☐ Yes ☐ No
9. Does the Applicant accept prepayments by clients for goods or services prior to delivery or performance of an agreement? ☐ Yes ☐ No
10. Does the Applicant have custody or control over any funds or money belonging to any of its clients, including escrow or trust accounts? ☐ Yes ☐ No  
*If Yes, describe the nature of the control or custody and the oversight procedures associated with protecting such funds or money:* \_\_\_\_\_
11. Does the Applicant have access to clients' financial systems (e.g.: accounting, payroll, purchasing systems, etc.)? ☐ Yes ☐ No  
*If Yes, describe the nature of the access and the oversight procedures associated with protecting such financial system access:* \_\_\_\_\_
12. Does the Applicant accept payment or funds transfer instructions from clients relating to refunds or repayment of goods, services, or funds held in the Applicant's custody? ☐ Yes ☐ No  
*If Yes, describe the communication methods by which such instructions are received (e.g. telephone, email, text message, Telefacsimile (fax), general mail, etc.):* \_\_\_\_\_
13. Does the Applicant confirm all payment or funds transfer instructions from a client by a direct call to the client using only the telephone number provided by the client before the payment or funds transfer instruction was received? ☐ Yes ☐ No  
*If Yes:*  
a. Is such callback procedure performed by an individual other than the individual who received the payment or funds transfer instruction? ☐ Yes ☐ No  
b. Does the Applicant confirm all such payments or funds transfer instructions made by a client with an individual at the client, other than the individual who initiated such payment or funds transfer instruction? ☐ Yes ☐ No  
c. Does the Applicant refrain from making any such payments or funds transfers until after the client has responded to the Applicant's inquiry regarding the authenticity of such payment or funds transfer instruction request? ☐ Yes ☐ No  
d. Does the Applicant require that all such payments or funds transfer instructions made by a client be approved by the supervisor of the individual who received the payment or funds transfer instruction, before it is acted upon? ☐ Yes ☐ No

### INTERNAL FUNDS-TRANSFER INSTRUCTION CONTROLS

---

14. Does the Applicant maintain a pre-established list of employees who are authorized to initiate payment or funds transfer requests for reasons other than a vendor invoice or a client repayment? ☐ Yes ☐ No  
*If Yes:*  
a. Does the Applicant have procedures in place to verify the authenticity of any payment or funds transfer request received by an authorized employee from an internal company source (e.g. another employee, subsidiary, location, or department)? ☐ Yes ☐ No  
*If Yes, describe such procedures:* \_\_\_\_\_

- b. Are all such procedures performed consistently across all subsidiaries, business units, departments, and locations? ☐ Yes ☐ No
15. Do payments or funds transfers of a certain amount require dual authorization? ☐ Yes ☐ No  
If Yes, what is that amount? \_\_\_\_\_
16. Does the Applicant require that any payment or funds transfer request made by an internal company source be approved by the supervisor of the individual who received the payment or funds transfer request, before it is acted upon? ☐ Yes ☐ No
17. Is the authority to make electronic funds transfers (e.g. wire transfers, ACH payments, etc.) limited by the amount of each transfer (for example: \$250,000 initiated by one employee and approved by a separate employee; \$500,000 initiated and approved by two separate employees; \$1,000,000 or more initiated and approved by a senior officer, such as the CEO, CFO, or President, etc.)? ☐ Yes ☐ No  
If Yes, what are the dollar amounts that trigger approval, and who has the authority to approve such amounts?  
\_\_\_\_\_
18. Are certain employees with authority to approve electronic funds transfers (e.g. wire transfers, ACH transfers, etc.) required to be available at all times by cell phone or other means? ☐ Yes ☐ No
19. Is there a limit on the number of electronic funds transfers (e.g. wire transfers, ACH payments, etc.) an employee can approve during a specified time period? ☐ Yes ☐ No  
If Yes, what is the number of transfers, and the time period applicable to such transfers?  
\_\_\_\_\_
20. Is there a limit on the total dollar amount of electronic funds transfers (e.g. wire transfers, ACH transfers, etc.) that can be approved by any one employee during a specified time period? ☐ Yes ☐ No  
If Yes, what is the dollar limit amount on transfers, and the time period applicable to such transfers?  
\_\_\_\_\_

If the Applicant answered No to any part of Questions 4-20, attach details.

## LOSS INFORMATION

21. Has the Applicant sustained any Computer or Social Engineering Fraud losses during the past three years? ☐ Yes ☐ No  
If Yes, attach details of such, including costs, losses, or damages incurred or paid, any corrective procedures to avoid such incidents in the future, and any amount paid as loss under any insurance policy.

## NOTICE REGARDING COMPENSATION

For information about how Travelers compensates independent agents, brokers, or other insurance producers, please visit this website: [http://www.travelers.com/w3c/legal/Producer\\_Compensation\\_Disclosure.html](http://www.travelers.com/w3c/legal/Producer_Compensation_Disclosure.html)

If you prefer, you can call the following toll-free number: 1-866-904-8348. Or you can write to us at Travelers, Agency Compensation, One Tower Square, Hartford, CT 06183.

## FRAUD STATEMENTS – ATTENTION APPLICANTS IN THE FOLLOWING JURISDICTIONS

**ALABAMA, ARKANSAS, DISTRICT OF COLUMBIA, MARYLAND, NEW MEXICO, AND RHODE ISLAND:** Any person who knowingly (or willfully in MD) presents a false or fraudulent claim for payment of a loss or benefit or who knowingly (or willfully in MD) presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

**COLORADO:** It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company to defraud or attempt 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 to defraud or attempt to defraud the policyholder or claimant regarding a settlement or award payable from insurance proceeds will be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

**FLORIDA:** 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.

**KENTUCKY, NEW JERSEY, NEW YORK, OHIO, AND PENNSYLVANIA:** 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. (In New York, the civil penalty is not to exceed five thousand dollars (\$5,000) and the stated value of the claim for each such violation.)

**LOUISIANA, MAINE, TENNESSEE, VIRGINIA, AND WASHINGTON:** It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company to defraud the company. Penalties include imprisonment, fines, and denial of insurance benefits.

**OREGON:** 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 may be guilty of a crime and may be subject to fines and confinement in prison.

**PUERTO RICO:** Any person who knowingly and intending to defraud presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, will incur a felony and, upon conviction, will be sanctioned for each violation with the penalty of a fine of not less than \$5,000 and not over \$10,000, or a fixed term of imprisonment for three years, or both penalties. Should aggravating circumstances be present, the penalty established may be increased to a maximum of five years; if extenuating circumstances are present, it may be reduced to a minimum of two years.

## **SIGNATURES**

The undersigned Authorized Representative represents that to the best of his or her knowledge and belief, and after reasonable inquiry, the statements provided in response to this Application are true and complete, and, except in NC, may be relied upon by Travelers as the basis for providing insurance. The Applicant will notify Travelers of any material changes to the information provided.

☐ Electronic Signature and Acceptance – Authorized Representative\*

\*If electronically submitting this document, electronically sign this form by checking the Electronic Signature and Acceptance box above. By doing so, the applicant agrees that use of a key pad, mouse, or other device to check the Electronic Signature and Acceptance box constitutes acceptance and agreement as if signed in writing and has the same force and effect as a signature affixed by hand.

Authorized Representative Signature: <b>X</b>	Authorized Representative Name, Title, and email address:	Date (month/dd/yyyy):
Producer Name (required in FL & IA): <b>X</b>	State Producer License No (required in FL):	Date (month/dd/yyyy):
Agency:	Agency contact and email address:	Agency Phone Number:

## **ADDITIONAL INFORMATION**