TRAVELERS

Travelers Casualty and Surety Company of America **Multi-Factor Authentication Attestation**

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 limits of liability will be reduced, and may be completely exhausted, by amounts paid as defense costs, and any retention will be applied against defense costs. The Insurer will not be liable for the amount of any judgment, settlement, or defense costs incurred after exhaustion of the limit of liability.

GENERAL INFORMATION

Name of Applicant:

Street Address:

City:	State:	Zip:

Applicant Website(s):

Multi-Factor Authentication

Multi-factor authentication refers to the use of two or more means of identification and access control—sometimes referred to as "something you know, something you have, or something you are." A username and password, for example, is something you know. Requiring a code sent via text message (SMS) establishes "something you have," i.e., a mobile phone belonging to you. Biometric authentication, through a fingerprint or retina scan, establishes "something you are." Multi-factor authentication is successfully enabled when at least two of these categories of identification are required in order to successfully verify a user's identity when accessing systems.

Multi-Factor Authentication for Remote Network Access

Requiring multi-factor authentication for remote network access is an important security control that can help reduce the potential for a network compromise caused by lost or stolen passwords. Without this control an intruder can gain access to an insured's network in a similar manner to an authorized user.

Multi-Factor Authentication for Administrative Access

Requiring multi-factor authentication for both remote and internal access to administrative accounts helps to prevent intruders that have compromised an internal system from elevating privileges and obtaining broader access to a compromised network. The existence of this control can prevent an intruder from gaining the level of access necessary to successfully deploy ransomware across the network.

Multi-Factor Authentication for Remote Access to Email

Requiring multi-factor authentication for remote access to email can help reduce the potential for a compromise to corporate email accounts caused by lost or stolen passwords. Without this control an intruder can easily gain access to a user's corporate email account. Threat actors often use this access to perpetrate various cyber crime schemes against the impacted organization and its clients and customers.

The controls described above and listed below are the minimum controls that must be in place in order to be eligible for a Cyber policy. Because of the importance of the controls in preventing ransomware attacks the following attestation should be completed with the assistance of the person(s) in charge of IT security. If IT security is outsourced to a managed security provider or other 3rd party please complete the attestation below with their assistance.

MULTI-FACTOR AUTHENTICATION ATTESTATION

1. Multi-Factor authentication is required for all employees when accessing email through a website or cloud based service. ☐ Yes ☐ No ☐ Email is not web based

2. Multi-Factor authentication is required for all remote access to the network provided to employees, contractors, and 3rd party service providers. ☐ Yes ☐ No

3. In addition to remote access, multi-factor authentication is required for the following, including such access provided to 3rd party service providers:
   a. All internal & remote admin access to directory services (active directory, LDAP, etc.). ☐ Yes ☐ No
   b. All internal & remote admin access to network backup environments. ☐ Yes ☐ No
   c. All internal & remote admin access to network infrastructure (firewalls, routers, switches, etc.). ☐ Yes ☐ No
   d. All internal & remote admin access to the organization's endpoints/servers. ☐ Yes ☐ No

4. The signer of this form has done so with the assistance of the person in charge of IT security. ☐ Yes ☐ No

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

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 Executive Officer 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 North Carolina 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 – Executive Officer

*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.

Executive Officer is defined as the applicant's chief executive officer, chief financial officer, chief information security officer, risk manager, in-house general counsel, or the functional equivalent.

Executive Officer Signature: **X**	Executive Officer Name and Title:	Date *(month/dd/yyyy)*:
Producer Name (required in FL & IA): **X**	State Producer License No (required in FL):	Date *(month/dd/yyyy)*:
Agency:	Agency contact and email address:	Agency Phone Number: