TRAVELERS

CyberRisk Social Engineering Fraud Supplement

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.

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

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: **X**	Authorized Representative Name, Title, and email address:	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:

ADDITIONAL INFORMATION