TRAVELERS

CyberRisk Payment Card 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:

UNDERWRITING QUESTIONS

1. Is the Applicant subject to the Payment Card Industry Data Security Standard (PCI-DSS)? ☐ Yes ☐ No
   If Yes:
   a. What level requirement?
   b. Which version?
   c. How many credit card transactions are processed in a typical year?
   d. Is the Applicant currently PCI compliant? ☐ Yes ☐ No
      If No:
      i. What percentage of compliance has been achieved?
      ii. When is full compliance anticipated?
      iii. When was the last PCI audit?
2. Is the Applicant a member of the retail ISAC? ☐ Yes ☐ No
3. Are employees trained to recognize signs of tampering to transaction terminals? ☐ Yes ☐ No ☐ N/A
4. Has the Applicant implemented a "White Listing" approach on its Point of Sale system? ☐ Yes ☐ No
5. Are critical patches for extreme risk vulnerabilities within the PCI environment applied within 30 days? ☐ Yes ☐ No
6. Is the Applicant's Point of Sale network segmented from any other company networks? ☐ Yes ☐ No
   If Yes, are segmentation controls tested on a regular basis? ☐ Yes ☐ No
7. Does the Applicant allow email or web browsing on Point of Sale networks? ☐ Yes ☐ No
8. Does the Applicant use any operating system for which software patches are no longer available or that are no longer supported by the vendor or manufacturer? ☐ Yes ☐ No
   If Yes, describe all compensating controls and plans to update the operating system:
9. Are shared credentials used to access Point of Sale or other systems? ☐ Yes ☐ No
10. Have all system credentials been changed from the default settings? ☐ Yes ☐ No
11. Do the Applicant's Point of Sale devices accept chip/PIN or chip/signature transactions? ☐ Yes ☐ No ☐ N/A
    If No, is there a plan to do so, and when will such plan be implemented?

12. Does the Applicant store consumer card data in its systems for future transactions? ☐ Yes ☐ No
If Yes, is this data encrypted? ☐ Yes ☐ No

13. Has the Applicant implemented end-to-end encryption in its Point of Sale system? ☐ Yes ☐ No
If Yes, describe the implementation: _____

14. Has the Applicant implemented tokenization in its Point of Sale system? ☐ Yes ☐ No
If Yes, describe the implementation: _____

15. Does the Applicant have an ecommerce site or mobile application? ☐ Yes ☐ No
If Yes:
    a. Is credit card data or other protected identity information stored in the Applicant's environment? ☐ Yes ☐ No
    b. Is ecommerce payment information encrypted or tokenized at all times? ☐ Yes ☐ No
    c. Is a hosted payment page utilized to accept online transactions? ☐ Yes ☐ No

16. Does the Applicant allow remote access to the POS network? ☐ Yes ☐ No
If Yes:
    a. Are vendors with remote access required to demonstrate adequate security controls? ☐ Yes ☐ No
    b. Are vendors specifically required to use unique passwords when accessing the Applicant's environment that are not utilized by the vendor at other client sites? ☐ Yes ☐ No
    c. Is two factor authentication required for remote access? ☐ Yes ☐ No
    d. Is access restricted to only necessary systems and applications on a business need basis? ☐ Yes ☐ No
    e. Is access logged and monitored for unusual activity? ☐ Yes ☐ No

17. Describe additional controls or procedures that may apply (white listing remote IP addresses, setting geographic or temporal login limitations, etc.):

18. What information security certifications are maintained by the Applicant (e.g.: PCI, ISO, SSAE16, etc.)?

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