TRAVELERS

Social Engineering Fraud/Funds Transfer Fraud
Supplemental Commercial Crime Application

Travelers Casualty and Surety Company of America

The term **Applicant** means all corporations, organizations or other entities, including subsidiaries and Employee Benefit Plans subject to ERISA, that are proposed for the crime insurance coverage to which Social Engineering Fraud coverage is requested to be attached.

I. GENERAL INFORMATION

1. Name of Applicant: _____

   Mailing Address: _____ City: _____ State: ___ ZIP: _____

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 ☐

II. VENDOR CONTROLS

(Attach a separate sheet to this Supplemental Application with an explanation for any "No" answers to questions in this Section II. or if additional space is needed to support the request for the Social Engineering Insuring Agreement.)

1. Does the Applicant verify the authenticity of all new 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 ☐
2. Does the Applicant have procedures in place to verify the authenticity of invoices and other payment requests received from a Vendor? Yes ☐ No ☐
3. 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 ☐
4. 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? *(If yes, please answer parts a, b, c., and d. below)*: Yes ☐ No ☐
   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(s) of the individual who received the change request, *before* it is acted upon? Yes ☐ No ☐
5. 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 ☐

III. CLIENT CONTROLS

(Attach a separate sheet to this Supplemental Application with an explanation for any "No" answers to questions in this Section III. or if additional space is needed to support the request for the Social Engineering Insuring Agreement.)

1. 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, please describe the procedures: _____

   _____

2. Are the procedures described in Question 1. above applicable for each and every transaction *prior* to furnishing goods or services to Clients? Yes ☐ No ☐

3. Does the Applicant accept prepayment by Clients for goods or services *prior to* delivery or performance of an agreement? Yes ☐ No ☐

4. Does the Applicant have custody or control over any funds or money belonging to any of its Clients, including but not limited to escrow or trust accounts? Yes ☐ No ☐

   If yes, please describe the nature of the control or custody and the oversight procedures associated with protecting such funds or money: _____

   _____

   _____

5. Does the Applicant have access to Clients' financial systems (e.g., accounting, payroll, purchasing systems, etc.)? Yes ☐ No ☐

   If yes, please describe the nature of the access and the oversight procedures associated with protecting such financial system access: _____

   _____

   _____

6. Does the Applicant accept payment or funds transfer instructions from a Client relating to a refund or repayment of goods, services or funds held in the Applicant's custody? Yes ☐ No ☐

   If yes, please describe the communication methods by which such instructions are received (e.g. telephone, e-mail, text message, telefacsimile (fax), general mail, etc.): _____

   _____

   _____

7. 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? *(If yes, please answer parts a., b., and c. below)*: Yes ☐ No ☐

   a. Is the call back procedure above 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 the payment 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 requests? Yes ☐ No ☐

8. Does the Applicant require that all such payments or funds transfer instructions made by a Client be approved by the Applicant's Supervisor(s) of the individual who received the payment funds transfer instruction, *before* it is acted upon? Yes ☐ No ☐

IV. INTERNAL FUNDS TRANSFER INSTRUCTION CONTROLS

(Attach a separate sheet to this Supplemental Application with an explanation for any "No" answers to questions in this Section IV. or if additional space is needed to support responses to the questions.)

1. Does the Applicant maintain a pre-established list of employees authorized to initiate payment or funds transfer requests for reasons *other than* a Vendor invoice, or a Client repayment? *(If yes, please answer parts a. and b. below.)*: Yes ☐ No ☐

   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, please describe such procedures: _____

      _____

   b. Are all such procedures performed consistently across all subsidiaries, business units, departments, and locations? Yes ☐ No ☐

2. Do payments or funds transfers of a certain amount require dual authorization? Yes ☐ No ☐

   If yes, what is that amount? _____

3. Does the Applicant require that any payment or funds transfer request made by an internal company source be approved by the Applicant's Supervisor(s) of the individual who received the payment or funds transfer request, *before* it is acted upon? Yes ☐ No ☐

4. Is the authority to make electronic funds transfers (wire transfers, ACH payments, etc.) limited by the amount of each transfer? (for example: $250,000.00 initiated by one employee and approved by a separate employee; $500,000.00 initiated and approved by two separate Employees; $1,000,000.00 or more initiated and approved by a senior officer such as the CEO, President, CFO, etc.) Yes ☐ No ☐

   If yes, what dollar amounts require additional approval before a transfer can be made, and what are the positions at each level and who must approve the transfer?

   _____

   _____

5. 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 ☐

6. Is there a limit on the number of electronic funds transfers (e.g., wire transfers, ACH transfers, etc.) an employee can approve during a specified time period? (24 hours, 48 hours, 72 Hours, 1 Week, etc.) Yes ☐ No ☐

   If yes, how many transfers and at what time interval?

   _____

7. Is there a limit on the total dollar amount of electronic funds transfers (wire transfer, ACH transfer, etc.) that can be approved by any one employee during a specified time period? (24 hours, 48 hours, 72 hours, 1 Week, etc.)? Yes ☐ No ☐

   If yes, what is that dollar amount limit and at what time interval?

   _____

V. LOSS INFORMATION

Has the Applicant sustained any Computer or Social Engineering Fraud losses during the past 3 years? Yes ☐ No ☐

If yes, please complete the following. Attach a separate sheet if more space is needed.

Date of Loss	Total Amount of Loss	Description of Loss and Corrective Action

VI. COMPENSATION NOTICE

Important Notice Regarding Compensation Disclosure

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, Enterprise Development, One Tower Square, Hartford, CT 06183.

VII. FRAUD WARNINGS

Attention: Insureds in Alabama, Arkansas, D.C., 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.

Attention: Insureds in 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.

Attention: Insureds in 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.

Attention: Insureds in 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.)

Attention: Insureds in Louisiana, Maine, Tennessee, Virginia, and Washington
It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines, and denial of insurance benefits.

Attention: Insureds in 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.

Attention: Insureds in Puerto Rico
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 dollars ($5,000) and not more than ten thousand dollars ($10,000), or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances be 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.

VIII. SIGNATURE SECTION

THE UNDERSIGNED OFFICER OF THE APPLICANT (AUTHORIZED REPRESENTATIVE) DECLARES THAT TO THE BEST OF HIS OR HER KNOWLEDGE AND BELIEF, AFTER REASONABLE INQUIRY, THE STATEMENTS SET FORTH IN THIS APPLICATION FOR INSURANCE, INCLUDING ANY SUPPLEMENTS OR MATERIALS MADE PART OF THIS APPLICATION, ARE TRUE AND COMPLETE AND MAY BE RELIED UPON BY TRAVELERS. IF ANY INFORMATION IN THIS APPLICATION, OR ANY SUPPLEMENTS OR MATERIALS SUBMITTED THEREWITH, CHANGES PRIOR TO THE INCEPTION DATE OF THE BOND THAT TRAVELERS MAY ISSUE TO THE APPLICANT, THE APPLICANT WILL NOTIFY TRAVELERS AND TRAVELERS MAY MODIFY OR WITHDRAW ANY

OUTSTANDING QUOTATION. TRAVELERS IS AUTHORIZED TO MAKE ANY INVESTIGATION OR INQUIRY IN CONNECTION WITH THIS APPLICATION.

THE SIGNING OF THIS APPLICATION DOES NOT BIND TRAVELERS TO OFFER, NOR THE APPLICANT TO PURCHASE, THE INSURANCE. IT IS AGREED THAT THIS APPLICATION, INCLUDING ANY SUPPLEMENTS OR MATERIALS MADE PART OF THIS APPLICATION, WILL BE THE BASIS OF INSURANCE, AND THAT TRAVELERS WILL HAVE RELIED UPON THIS APPLICATION, INCLUDING ANY SUPPLEMENTS OR MATERIALS MADE PART OF THIS APPLICATION, IN ISSUING THE BOND.

ELECTRONICALLY REPRODUCED SIGNATURES WILL BE TREATED AS ORIGINAL.

Signature*: Officer of **Applicant**
(Authorized Representative)

Name (Printed)

Title

Date

***IF YOU ARE ELECTRONICALLY SUBMITTING THIS APPLICATION TO TRAVELERS, APPLY YOUR ELECTRONIC SIGNATURE TO THIS FORM BY CHECKING THE ELECTRONIC SIGNATURE AND ACCEPTANCE BOX BELOW. BY DOING SO, YOU HEREBY CONSENT AND AGREE THAT YOUR USE OF A KEY PAD, MOUSE, OR OTHER DEVICE TO CHECK THE ELECTRONIC SIGNATURE AND ACCEPTANCE BOX 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.**

AUTHORIZED REPRESENTATIVE'S ELECTRONIC SIGNATURE AND ACCEPTANCE ☐

IX. PRODUCER INFORMATION (ONLY REQUIRED IN FLORIDA, IOWA, AND NEW HAMPSHIRE):

Producer Signature

Producer Name (Printed)

Agency Name

Agency Code

License Number

Vendor Email Hacked

Coverage: Crime Insurance

Cause of action: Social Engineering Fraud

Type of organization: Private Company

Number of employees: Less than 250

Annual revenue: Less than $250 million

The controller for a distributor of component parts was responsible for making regular payments to overseas vendors from which the distributor purchased products for resale in the United States. After many months of working with one particular vendor and receiving regular shipments, the controller received an email that appeared to come from his vendor contact, indicating that the vendor's bank was having issues with accepting payments, and asking if the next payment could be made to a new bank. Due to the vendor's overseas location, verification was a challenge. After the supposed vendor applied some pressure, the controller paid the invoice via wire transfer.

Resolution: **The following month, when the real vendor realized that its best customer's payment was overdue, an investigation determined that the vendor's email had been hacked, and an imposter had been socially engineering the company into believing that the change in bank information was authentic. In the end, the fraudster finagled almost $250,000 from the distributor.**

Fake CEO Scam

Coverage: Crime Insurance

Cause of action: Social Engineering Fraud

Type of organization: Public Company

Number of employees: More than 250

Annual revenue: More than $150 million

The regional CFO of a subsidiary of a large, publically traded company received an email purporting to be from the assistant to the CEO in the United States. The email requested that the CFO transfer a large sum of money immediately to facilitate covering a tax payment in China. When the CFO questioned the request, a follow-up phone call was made to the CFO, assuring him that the proper authority was granted and that it had come "from the highest levels" within the organization. With intimate knowledge of company policies, and an official looking letter on company letterhead "authorizing" the transfer, the CFO transferred the money by wire. The scam was detected after another attempt at transferring funds was stopped by the subsidiary's bank.

Resolution: **After recovering only a portion of the original wire transfer, the subsidiary suffered a $1 million loss.**

Illegitimate Client

Coverage: Crime Insurance
Cause of action: Social Engineering Fraud
Type of organization: Private Company
Number of employees: Less than 50
Annual revenue: Less than $100 million

A business manager handling bill payment and bookkeeping services for a client received an email, purportedly from a client, inquiring about her balance and availability of funds for a wire transfer. The email included details regarding the scope of services that were provided, as well as information about other transactions that had recently been performed. The wire, for $100,000, was to go to an offshore account, purportedly for the purchase of a new piece of real estate. After the purported client won the business manager's trust, the business manager authorized wiring the funds to the fraudster's account.

Resolution: **After noticing some activity in the client's spam account, the client grew suspicious and contacted its bank, requesting that the wire be stopped. Unfortunately, the wire had been sent and all $100,000 was lost.**

Something for Nothing?

Coverage: Crime Insurance
Cause of action: Social Engineering Fraud
Type of organization: Law Firm
Number of employees: Less than 200
Annual revenue: Less than $100 million

A regional law firm received a request to sign up a new client from overseas. The new client wished the firm to pursue a debtor in the United States who was delinquent on its bills. The client explained that it would pay the retainer and entered into an agreement with the law firm. During the vetting process, the client informed the firm that the debtor had agreed to pay the bill, but had already written the check to the law firm. The client instructed the law firm to cash the official looking cashier's check that had just arrived, deduct its fee, and wire the remainder to the client.

Resolution: **The check provisionally cleared the client's bank, but because of effective routing, the hold expired after the firm had already wired out the funds. The fraud was detected when the check bounced, and the fraudster was long gone. All $250,000 was lost, as the wire could not be recalled.**

To Learn More

Contact your Chubb Crime Insurance underwriter or visit us online.

Form 14-01-1140 (Ed. 7/14)