

Fraudulently Induced Transfer Supplemental Application

Nearly all Fraudulently Induced Transfer losses arise from one or more of your employees being tricked into believing that a request to modify account information, transfer funds or initiate a payment to a third party is genuine. The fraudster may use hacked legitimate email addresses, email addresses designed to look real but which actually contain anomalies, phone calls or even in-person meetings to impersonate a client, vendor or another employee. These questions are designed to help Intact Public Entities understand the extent to which your organization is prepared to defend against these types of frauds.

NOTE: This application must be completed in addition to the Comprehensive Dishonesty, Disappearance and Destruction All sections must be completed
Answers must be provided for all entities, including subsidiaries that are shown on (or proposed for) the crime insurance coverage to which this Fraudulently Induced Transfer coverage is being requested

General Information

Policy Number _____
 Legal Name of Applicant _____
 Mailing Address _____ Postal Code _____
 Key Broker Contact _____
 Brokerage Name _____
 Phone _____ Email _____
 Applicant's operations (including activities, programs, events, U.S. or International exposures) _____

Limits of Insurance Requested

\$10,000 \$25,000 \$50,000 \$100,000 Over \$100,000 indicate limit \$ _____

Personnel Information

Please indicate the number of people (including volunteers) that handle money, have signing authority and are responsible for wire transfers _____

Fraudulently Induced Transfer Procedures

Are all employees who are responsible for authorizing and executing payments or funds transfer requests provided anti-fraud training? YES _____ NO _____
 Are all employees who are custodians of or have access to sensitive/private information provided anti-fraud training? YES _____ NO _____
 Does the anti-fraud training include fraudulently induced transfer losses, phishing, masquerading, and other types of fraud schemes? YES _____ NO _____
 Is there a formalized process in place which an employee can flag or otherwise bring to the attention of management potential fraudulently induced transfers or other types of fraudulent activity (e.g. phone hotline, dedicated reporting email address, intranet based reporting)? YES _____ NO _____
 If "YES", please describe the procedures _____

Vendor or Supplier Controls

Are there procedures in place to verify the authenticity of all new vendors prior to transacting business with them? YES _____ NO _____
 If "YES", please describe the procedures _____

Are there procedures in place to verify the authenticity of invoices and other payment requests received from a vendor? YES _____ NO _____

Is every request to change vendor or supplier account information (including all bank account information, invoice changes, telephone or telefacsimile numbers, location and contact information) confirmed prior to implementation by a direct call to the vendor or supplier using only the telephone number provided by the vendor or supplier before the change request was received? YES _____ NO _____

Are all changes to the vendor or supplier information required to be approved by a second, next-level person prior to the change being made? YES _____ NO _____

Client Controls

Are there procedures (e.g. credit/background checks, physical location information, bank account information) in place to verify the authenticity of all prospective clients prior to providing any goods or services? YES _____ NO _____

If "YES", please describe the procedures _____

Are these procedures (noted above) used without exception? YES _____ NO _____

If "NO", provide full details _____

Do you have custody or control over any funds or money belonging to any of your clients, including but not limited to escrow or trust accounts? YES _____ NO _____

If "YES", provide full details regarding the nature of the control or custody and the oversight procedures associated with protecting such funds or money: _____

Funds Transfer Procedures

Does your company transfer funds by Wire _____ Internet _____ Voice _____ Other _____

If "Other" please specify _____

If any of the methods above have been checked, for each item please state the following:

	Wire	Internet	Voice	Other
Estimated frequency	_____	_____	_____	_____
Average dollar amount of each transfer	\$ _____	\$ _____	\$ _____	\$ _____
Maximum dollar amount of any one transfer	\$ _____	\$ _____	\$ _____	\$ _____

Are there procedures in place to ensure that all payment or funds transfer requests are authentic? YES _____ NO _____

Do payments or funds transfers require dual authorization at all times? YES _____ NO _____

If "NO" provide full details _____

For transfers requested by any internal company source do you require approval by the supervisor (of the person who received the transfer request) before the transfer is acted upon? YES _____ NO _____

Is the authority to make electronic funds transfers (wire transfers, ACH payments, etc.) limited by the amount of each transfer?

Example: \$250,000.00 is 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", provide the following details

What dollar amounts require additional approval before a transfer can be made \$ _____

What are the positions at each level _____

Who must approve the transfer (indicate positions) _____

Describe any other procedures or controls in place to minimize the frequency or severity of a potential fraud loss

Example: Limitations on the number of transfers a person may make in a given time period, maximum dollar value a person may transfer in a given time period, use of third party software etc.

Losses

Provide details of all losses in the past six (6) years for all entities under the terms of this coverage (whether or not insured)

Check if none _____

Date of Loss	Amount of Loss	Description of Loss (add sheet if necessary)	Corrective Measure(s) Taken (add sheet if necessary)
	\$		
	\$		
	\$		
	\$		

Applicant Acknowledgement

The undersigned authorized officer of the organization declares that, to the best of his/her knowledge, the statements set forth herein are true. Signing of this application does not bind the Insurer to offer, nor the applicant to accept Insurance, but, it is agreed that this form shall be the basis of the contract should a policy be issued, and this form will be attached to and become part of the policy.

The undersigned, on behalf of the insured organization, acknowledges that any personal information provided in connection with this application (including but not limited to the information contained in this form) has been collected in accordance with applicable privacy legislation and this information shall only be used or shared by the Company to assess, underwrite and price insurance products and related services, administer and service insurance policies, evaluate and investigate claims, detect and prevent fraud, analyze and audit businesses results and/or comply with regulatory or legal requirements.

Applicant Name _____ **Title/Position** _____
Applicant Signature _____ **Date** _____
Broker Name _____
Broker Signature _____