THEODORE LIFTMAN INSURANCE, INC.
FINANCIAL INSURANCE
ESTABLISHED 1957
Liftman Insurance Agency (NY, CA) Liftman Ins Agency Co (NC)

FIDELITY BOND APPLICATION FOR INVESTMENT ADVISORS

APPLICATION

Name of Insured:_____
(*First Named Insured and all additional insureds. Attach separate sheet if necessary*)

Principal Address: _____

Year Established:_____ **Effective Date of Coverage:**_____

Referred by
☐ Fidelity Investments ☐ Schwab ☐ Other_____

1) **Description of Organization**
☐ Partnership ☐ Corporation ☐ Proprietorship ☐ LLC

2) **Do you currently have a Fidelity Bond?** ☐ Yes ☐ No (If yes, please complete the following.)

Insurance Carrier	Limit of Insurance	Deductible	Expiring Premium

Has any similar insurance been declined or cancelled during the past three years? ☐ Yes ☐ No
If yes, please explain: _____
_____

3) **Loss Experience** (during the past 3 years) ☐ Check if none
Please provide a list of all losses sustained during the past three years, reimbursed or not.
_____

4) **Classification of Employees**
Total number of employees: _____ Total number of independent contractors: _____

5) **Location Information**
Number of additional locations: _____

6) **Audit & Internal Control Procedures**
A. Is an independent CPA firm involved in the applicant's financial reporting? ☐ Yes ☐ No
If yes, what is the level of reporting? ☐ Audit ☐ Review ☐ Compilation
B. Do you ever take physical custody of your clients' assets? ☐ Yes ☐ No
C. Who furnishes your clients with statements of account activities?_____
How frequently?_____
D. Have you ever committed or been charged with SEC disciplinary violations? ☐ Yes ☐ No
If yes, please attach a statement providing full details.

E. Are bank accounts reconciled by someone not authorized to deposit or withdraw? ☐ Yes ☐ No
If no, please explain alternative controls: _____

F. Is countersignature of checks required? ☐ Yes ☐ No
If yes, limit countersignature is required: _____
If no, please explain alternative controls over check signing: _____
_____

G. Have there been any changes to ownership or management within the past three years? ☐ Yes ☐ No

H. Are internal controls systems designed so that no employee can control a process from beginning to end (e.g. request a check, approve a voucher and sign it)? ☐ Yes ☐ No
If no, please explain alternative controls: _____
_____

7) Pre-employment Screening (conducted prior to hiring in all business units)

A. Do you perform criminal background checks? ☐ Yes ☐ No

B Do you perform reference checks that include prior employers of the past five years? ☐ Yes ☐ No

8) Payroll Controls

A. Do you outsource your payroll function? ☐ Yes ☐ No

B. Are management policies and computer system controls in place to prevent persons who approve new hires from adding them into the payroll? ☐ Yes ☐ No

9) Purchasing

A. Is an authorized vendor list used and updated at least annually? ☐ Yes ☐ No

B. Are procedures in place to verify the existence and ownership of all new vendors prior to adding them to the authorized vendor list? ☐ Yes ☐ No

10) Computer & Funds Transfer Controls

A. Is there a software security system in place to detect fraudulent computer usage by employees or outsiders? ☐ Yes ☐ No

B. Are passwords and access codes changed at regular intervals and when users are terminated ☐ Yes ☐ No

C. Is there a written policy regarding wire transfers? ☐ Yes ☐ No

11) Fraudulent Transfer Instructions

A. Do you have written and documented procedures which are provided to your employees, whereby your employees that process wire transfers are to never process an internal request:

1. Unless the request comes from someone with documented authority and within their established dollar threshold? and ☐ Yes ☐ No
2. Without first validating the request with a call back to the requestor (inclusive of any owner) at a pre-determined work phone number? ☐ Yes ☐ No

If "No" to either of the above, please explain your procedures for authenticating an internal wire transfer request. _____
_____
_____

B. Do you provide social engineering training on at least an annual basis to employees that have wire transfer or accounts payable authority that educates them on:

1. How to detect and identify social engineering scams where a fraudulent email or phone call from a purported vendor or client is received, requesting their vendor or client bank account information be changed? ☐ Yes ☐ No

2. How to detect and identify social engineering scams where a fraudulent email or phone call from a purported owner or employee of yours is received, requesting a wire transfer be made on their behalf? ☐ Yes ☐ No

If "No", what kind of training do you provide to help them identify these types of fraudulent schemes and how often? _____

_____

_____

C. Do you authenticate all requested changes to client information (such as bank account, routing number, contact information) with a phone call to an authorized representative of the client at a phone number provided at the time of contracting? ☐ Yes ☐ No

D. Do you have a written policy regarding wire transfers from clients' accounts? ☐ Yes ☐ No

E. Have approval authorities been established in writing and are they current? ☐ Yes ☐ No

F. Has separation been established between the individuals responsible for approving and processing wire transfers? ☐ Yes ☐ No

G. Do you accept funds transfer instructions from clients or customers over the telephone, email, text message or similar method of communication? ☐ Yes ☐ No

If "Yes" do you have written and documented procedures in place which are provided to your employees and which require employees to authenticate such instructions? (Check all that apply):

1. By calling the customer or client at a predetermined phone number? ☐ Yes ☐ No
2. By sending a text message to a predetermined number? ☐ Yes ☐ No
3. By requiring a secret code or other method of identification known only to the customer/client to confirm identity? ☐ Yes ☐ No

If "No" to all of the above, please explain how you authenticate funds transfer instructions from clients or customers?_____

_____

_____

H. Do you require that all instructions are received by an employee specifically authorized to receive and act upon such instructions? ☐ Yes ☐ No

It is understood that the first premium upon the Policy applied for, and subsequent premiums thereon, are due at the beginning of each premium period, that the Underwriter is entitled to additional premiums because of any unusual increase in the number of Employees or Premises and that the Applicant agrees to pay all such premiums promptly. The Employees of the Applicant have all, to the best of the Applicant's knowledge and belief, while in the service of the Applicant always performed their respective duties honestly. There has never come to its notice or knowledge any information which in the judgment of the Applicant indicates that any of the said Employees are dishonest. Such knowledge as any officer signing for the Applicant may now have in respect to his own personal acts or conduct unknown to the Applicant, is not imputable to the Applicant.

KENTUCKY FRAUD WARNING: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance 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.

MINNESOTA FRAUD WARNING: A person who submits an application or files a claim with intent to defraud or helps commit a fraud against an insurer is guilty of a crime.

NEW JERSEY FRAUD WARNING: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

NEW YORK FRAUD WARNING: 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 shall also be subject to a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

OHIO FRAUD WARNING: Any person who, with intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

PENNSYLVANIA FRAUD WARNING: 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.

FLORIDA FRAUD WARNING: 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.

Application completed by (Name and Title): _____

Date: _____ Signature: _____

DESCRIPTION OF COVERAGES

This is a general description of coverages that may be included in a Fidelity Bond. Please refer to actual policy and endorsements for complete terms and conditions, which can be furnished upon request.

1. **Employee Theft**
   Covers loss of or damage to money, securities and other property resulting directly from theft committed by an employee. (This Insuring Agreement includes forgery committed by an employee which results in theft of money, securities or other property.)

THE FOLLOWING COVER ACTS COMMITTED BY SOMEONE OTHER THAN AN EMPLOYEE.

2. **Forgery or Alteration**
   Covers loss from forgery or alteration of checks, drafts, promissory notes, or similar written promises, orders or directions to pay a sum in money.

3. **Inside The Premises – Theft of Money and Securities**
   Covers loss of Insureds money and securities by theft, disappearance or destruction and damage to a locked safe, vault, cash register, cash box or cash drawer located inside the premises resulting from an actual or attempted theft of or unlawful entry into those containers. Also extend to loss from damage to the exterior of the premises resulting directly from an actual or attempted theft of money and securities. (This applies only if the Insured is the owner of the premises or the insured is liable for damage to it).

4. **Inside The Premises – Robbery Or Safe Burglary Of Other Property**
   Covers loss of or damage to other property resulting directly from robbery (or attempted) of a custodian or from robbery (or attempted) of a safe or vault that is within the Insureds premises.

5. **Outside The Premises**
   Covers loss of money and securities, outside the premises, in the care and custody of a messenger or an armored car resulting from theft, disappearance or destruction. Regarding loss of other property, this will cover losses to other property, outside the premises, in the care and custody of a messenger or an armored motor vehicle company resulting from a robbery.

6. **Computer Fraud**
   Covers loss of or damage to “funds” or “Other Property” resulting directly from an unauthorized transfer of “funds” or “Other Property” by a natural person who has gained unauthorized access to your “computer system.” (“Funds” and “Other Property” are defined terms within the policy). The typical scenario is where a hacker gains unauthorized access to the computer of the Insured and causes a fraudulent transfer resulting in a loss of “funds” or "Other Property”.

7. **Funds Transfer Fraud**
   Covers loss of funds by a "fraudulent instruction" directing a financial institution to transfer, pay or deliver funds from the Insured’s account (an account at a financial institution that is maintained by the Insured from which the Insured can transfer or make payments from. This includes electronic, cable, fax or telephone instructions or written instructions fraudulently purporting to be the Insured but which was in fact fraudulently transmitted by someone else without the insured’s knowledge or consent.

8. **Money Orders and Counterfeit Money**
   Covers loss resulting from your having accepted in good faith, in exchange for merchandise, money or services: a. money orders that are not paid upon presentation or b. counterfeit paper currency that is acquired during the regular course of business.

9. **Funds Transfer – False Pretenses Coverage**
   Provides coverage for the financial losses arising from social engineering fraud (phishing, spear phishing, pretext, and impersonation) perpetrated by email, instant message, text, telephone or other electronic means. It is where a fraudster impersonates a trusted business partner, vendor, employee or client by phone, email, or text, and tricks the Insured into voluntarily transferring funds to them.

   Claims examples:

   i. A CFO working remotely apparently sent an email request to the controller for a $143,000 wire transfer to a trusted vendor, a routine procedure. After completing the transfer, they discovered a fraudster had spoofed the CFO’s address, and had been conned.

   ii. A fraudster created fake email addresses for a VP of Finance and one of their suppliers that were off by just one character, and not noticed by either party. After an email exchange through the fake addresses, the VP of Finances transferred a $1,320,000 payment to the supplier account provided in the email, which turned out to be a fake account in China