STARR COMPANIES FRAUDULENT IMPERSONATIONS COVERAGE QUESTIONNAIRE

Insured Name: *Click here to enter text.*
Insured Web Site(s):

SECTION 1	
Are all wire transfers subject to at least three steps including (a) initiation (b) approval (3) release, and, are these steps completed by two or more authorized individuals?	Yes ☐No☐
Are all Company initiated ACH and similar transfers subject to at least two steps including (a) initiation (b) release?	Yes ☐No☐
Is a call-back, email, text or similar notification process in place within 24 hours for all electronic transfers of funds?	Yes ☐No☐
Does the notification go to an individual, other than any person involved in the initiation, approval or release of any wire transfer, ACH or similar transaction?	Yes ☐No☐
Does/do the Company's banking partners require independent approval of new user access?	Yes ☐No☐
Does the Company require second level internal approval of new user access?	Yes ☐No☐
Do all changes to user profiles require independent approval?	Yes ☐No☐
Do all changes to user profiles require second level internal approval?	Yes ☐No☐
Are daily alerts received/reviewed for any vendor, supplier or customer attempting to initiate an external ACH payment	Yes ☐No☐
Is a weekly (or more frequent) review of transfers, ACH payments or similar transactions greater than $10,000 conducted to validate proper support exists and payment is appropriate?	Yes ☐No☐
Does/do the Company's banking partners report of "one time" users or alternate payees?	Yes ☐No☐
Does the Applicant provide guidance and periodic anti-fraud training to employees concerning the detection of phishing and other social engineering scams? If so, please state the date of the last training and provide a copy of any related written materials (e.g. presentations)	Yes ☐No☐
Does the Company utilize firewall technology at all Internet points-of-presence to thwart unauthorized access?	Yes ☐No☐
Does the Company use antivirus software on all desktops and portable computers?	Yes ☐No☐
SECTION 2	
Has the Company ever sustained a significant system intrusion, data destruction or loss, virus, hacking or similar incident?	Yes ☐No☐
Has the Company identified any actual or attempted intrusions into its email systems?	Yes ☐No☐
Has the Company ever sustained any actual or attempted fraudulent transfer of funds from its accounts (including any event where the financial institution reimbursed or otherwise provided protection to the Company for the loss)?	Yes ☐No☐

For any "No" answers in Section 1 above, provide a detailed description of the alternate controls that are in place to prevent/detect fraudulent activities.

For any "Yes" answers in Section 2 above, provide a detailed description of the incident and describe the controls implemented to prevent/detect a recurrence of the same.

Signature of Applicant:	Date: