

PO Box 29502 #69121 | Las Vegas, NV 89126-9502 | (858) 618-1648 | Fax (858) 618-1655 | www.cresinsurance.com

Contact Person: _____ Email: _____ Phone: _____

Named Insured: _____ FEIN#: _____

Address: _____ City, State, Zip: _____

Total Gross Commission Income: _____ Gross Profit/Net Revenue: _____ Total # Employees: _____

☐ YES ☐ NO Within the past 5 years, has the Named Insured suffered any cyber incidents?
 IF YES, Explain: _____

☐ YES ☐ NO Are you aware of any circumstances that could give risk to a claim under a cyber-insurance policy?
 IF YES, Explain: _____

☐ YES ☐ NO Does your organization have a Designated Information Security Contact?*

☐ YES ☐ NO Does your organization provide mandatory information security training to all employees at least annually?
 If not, are they willing to implement it during the policy period?*

☐ YES ☐ NO Does the organization encrypt emails, mobile and computing devices containing sensitive information (e.g., PII, PHI, PCI) sent to external parties?

☐ YES ☐ NO Does Named Insured collect, process, store, transmit, or have access to any Payment Card Information (PCI), Personally Identifiable Information (PII), or Protected Health Information (PHI) other than employees of Named Insured?

IF YES:

Estimated annual volume of payment card transactions (credit cards, debit cards, etc.)? _____

How many PII or PHI records does Named Insured collect, process, store, transmit, or have access to? _____

☐ YES ☐ NO Does the organization have sensitive information stored on the cloud?*

How often does your organization apply updates to critical IT-systems and applications?*

☐ Weekly ☐ Monthly ☐ Quarterly ☐ Bi-Annually

If your organization performs back-ups, please select all that apply. Back-ups are:

☐ Encrypted ☐ Tested ☐ Online or Designated Cloud-Based ☐ Other

☐ YES ☐ NO Does the Named Insured maintain at least weekly backups of all sensitive or otherwise critical data and all critical business systems offline or on a separate network?

☐ YES ☐ NO Do you enforce Multi-Factor Authentication (MFA) for all employees, contractors, and partners?

☐ YES ☐ NO Does your organization have an incident response plan - tested and in-effect - setting forth specific action items and responsibilities for relevant parties in the event of cyber incident or data breach matter?

☐ YES ☐ NO Does the Named Insured require a secondary means of communication to validate the authenticity of funds transfer (ACH, wire, etc.) requests before processing a request in excess of \$25,000?

☐ YES ☐ NO Within the last 3 years has the Named Insured been subject to any complaints concerning the content of its website, advertising materials, social media, or other publications?

☐ YES ☐ NO Does the Named Insured enforce procedures to remove content (including third party content) that may infringe or violate any intellectual property or privacy right?

Signature: _____ Name: _____ Date: _____