

## APPENDIX A SOCIAL ENGINEERING FRAUD QUESTIONNAIRE

### COMPLETING APPENDIX A

- This document attaches to the Cyber Liability Insurance Application Form and the answers provided on this document
- Please read the enclosed Important Notices on the Proposal Form.
- Please answer all questions giving full and complete answers. It is important that all information is clear, factual and no information that could affect insurance terms is withheld.
- Where there is insufficient space to answer a question please answer on an attached separate sheet.
- Blanks and/or dashes, or answers 'known to insurers or brokers' or 'N/A' are unacceptable and may delay placement of your insurance.
- Upon completion, please print, sign and date the form before sending back to Marsh.
- If you have any doubts about completing this document, please contact Marsh.
- Provision of the Social Engineering Fraud extension of cover is subject to insurer review and acceptance of the answers in this document. Any unsatisfactory answers will lead to standard underwriting review, which may result a different additional premium rate to what has been quoted.

1. Does a Social Engineering Fraud risk management strategy exist and has the Applicant informed and alerted relevant staff at all locations of Social Engineering Fraud? Social Engineering Fraud includes Fake President Fraud, Payment Diversion Fraud and Customer/Management Impersonation Fraud.  Yes  No
2. Does the Applicant have a process in place at all locations where all unusual payment instructions purporting to come from the Applicant's senior management are followed up by call backs to senior management at a previously known and pre-designated phone number to confirm payment instructions and check authenticity?  Yes  No
3. Does the Applicant have a process in place at all locations where requests for authentication of bank account details or for information on bank account details purporting to come from bank officials are raised with the Applicant's senior management and followed up with previously known bank contacts to confirm authenticity of such requests?  Yes  No
4. Does the Applicant have a process in place at all locations where instructions to change bank account details purporting to come from vendors and suppliers are followed up by call backs to vendors and suppliers at a previously known and pre-designated phone number to confirm instructions to change bank account details and check authenticity?  Yes  No
5. Does the Applicant have a process in place at all locations where senior management approval is always required before a change to vendor and supplier bank account details is processed, such approval being given after review of the underlying request and the record of its verification?  Yes  No
6. Does the Applicant have a process in place at all locations where all bank statements are independently reconciled by persons not authorised to deposit or withdraw funds, issue funds transfer instructions or dispatch funds to customers?  Yes  No
7. Does the Applicant's email server and/or internet service provider (ISP) use any authentication methods at all locations? If Yes, please list:  Yes  No

8. Does the applicant use a third party software product to enhance email authentication procedures at all locations? If Yes, please list:  Yes  No

Use this space to comment on what other controls the Applicant applies to any questions where the answer is No:

## G. Declaration

**PLEASE NOTE: SIGNING THE DECLARATION DOES NOT BIND THE PROPOSER NOR THE INSURER TO COMPLETE THIS INSURANCE.**

The Proposer completing this Questionnaire represents that every effort has been made to facilitate the proper and accurate responses given in completion of this Application Form and confirms that the statements and particulars given are true and complete and that no material facts have been omitted, misstated or suppressed. The Proposer agrees that should any of the information given alter between the date of this Questionnaire and the inception date of the insurance to which this Questionnaire relates, they will give immediate notice thereof to Marsh and/or the insurer in writing, and acknowledges that the insurer may withdraw or modify any outstanding quotations and/or authorisation or agreement to bind insurance.

The Proposer acknowledges receipt of the Important Notices contained in the Application Form and that they have read and understood the content of them.

The Proposer consents to Marsh and insurers collecting, using and disclosing personal information as set out in the Privacy Collection Notice in the Important Notices contained in this Questionnaire.

The Proposer confirms that they are authorised by the Policyholder (and its partners/principals/directors if applicable) applying for this insurance to complete this Proposal Form and to accept the quotation terms for this insurance on behalf of the Policyholder (and its partners/principals/directors if applicable) applying for this insurance.

Full Name: \_\_\_\_\_ Position \_\_\_\_\_

Signature: \_\_\_\_\_ Date: DD/MM/YYYY

ONCE COMPLETED, PLEASE RETURN THIS FORM ALONG WITH THE CYBER LIABILITY APPLICATION FORM TO [cyberviclegalpractitioners@marsh.com](mailto:cyberviclegalpractitioners@marsh.com)