CYBER LIABILITY QUESTIONNAIRE

A. General

IIAC Member Firm Name: _____

Contact Name: _____

Office Address: _____

Website: _____

B. Financial Information

Revenue ($CDN):	Prior Fiscal Year	Current Fiscal Year	Projected for Next Fiscal Year

Are there any planned mergers, acquisitions or divestitures in the next 12 months? Yes ☐ No ☐

**if yes, please attach details of any due diligence done with respect to the new firms cyber practices, controls etc., on a separate page.*

C. Employees

1. How many offices/branches does your company operate? _____
2. How many employees work for the company? _____
3. How many registered representatives work for the company? _____
4. When your company hires a new representative, what due diligence is performed?

_____

D. Data Management

1. Is personally identifiable information (financial, bank, health related, etc.) encrypted by your company? Are entire records encrypted or only certain parts of records?

_____

**if only at certain times or if alternate safeguards are in place, please attach details on a separate page.*

2. How many personally identifiable records does the company own? _____
3. How often is the spear phishing training completed? _____

4. Has the company designated a Chief Information Security Officer?

   If 'No', who performs this function?

5. How many IT staff does the company have? _____

   If outsourced, please note: _____

6. Is training in place for employees as it relates to data breaches? Yes ☐ No ☐

E. Internal Controls/Processes

1. Does the company have the following in place:
   - Information Security Policy? Yes ☐ No ☐ ○ Cyber security failure and/or privacy breach incident response plan? Yes ☐ No ☐ ○ Penetration/Vulnerability Testing? Yes ☐ No ☐ ○ Intrusion Detection System? Yes ☐ No ☐ ○ Business Continuity Plan? Yes ☐ No ☐ ○ Information back-up protocols? Yes ☐ No ☐
   - How often are cyber security failure and privacy breach response table top exercises performed?

     _____

2. How long would it take to restore operations after a cyber security failure or a privacy breach event if one were to occur? _____

3. Is the board of directors involved in establishing the organization's cyber policies? Yes ☐ No ☐

4. Is the board of directors briefed on any critical cyber risks to the organization? Yes ☐ No ☐

5. Is your organization Payment Card Industry Data Security Standard (PCI DSS) compliant? Yes ☐ No ☐

6. What level (if no credit card transactions are ever processed, and therefore not applicable, please note):

   _____

F. Third Parties

1. Please provide a list of third parties and the functions they perform for your organization (including but not limited to cloud service providers, cyber security and privacy services providers):

   _____

2. Is due diligence done or is verification of security obtained with respect to third parties who you share private/personal information with?

   _____

3. Do you require indemnification in the event a third party experiences a cyber security breach and/or security failure which exposes PII owned by you and shared with such third party? Yes ☐ No ☐

   If no, what is their obligation to your company?

Please note that the content of this questionnaire is for indication purposes only and further details may be required in order to bind coverage.