

FinTech

Idea

Combined Liability Insurance for Financial Technology Companies

Technology

INNOVATION

Research

Creativity

Improvement

Concept

Proposal Form

All questions must be answered giving full and complete answers.
Please ensure that this Proposal Form is Signed and Dated.
All fee or turnover declarations to be in Australian Dollars.

LAUW

LONDON AUSTRALIA UNDERWRITING



IMPORTANT NOTICES

Utmost Good Faith

In accordance with Section 13 of the Insurance Contracts Act 1984, the policy of insurance is based on utmost good faith requiring Underwriter(s) and the proposer/insured(s) to act towards each other with the utmost good faith in respect of any matter relating to the insurance contract.

Your Duty of Disclosure

Before you enter into an insurance contract, you have a duty to tell **Underwriters** anything that you know, or could reasonably be expected to know, may affect **Underwriters** decision to insure you and on what terms.

You have this duty until **Underwriters** agree to insure you.

You have the same duty before you renew, extend, vary or reinstate an insurance contract.

You do not need to tell **Underwriters** anything that:

- reduces the risk **Underwriters** insure you for; or
- is common knowledge; or
- **Underwriters** know or should know as an insurer; or
- **Underwriters** waive your duty to tell **Underwriters** about.

If You Do Not Tell Underwriters Something

If you do not tell **Underwriters** anything you are required to, **Underwriters** may cancel your contract or reduce the amount **Underwriters** will pay you if you make a claim, or both.

If your failure to tell **Underwriters** is fraudulent, **Underwriters** may refuse to pay a claim and treat the contract as if it never existed.

Claims Made

Insuring Clause 1 (Professional Indemnity) and Insuring Clause 3a (Cyber Liability) operate on a **claims** made and notified basis. This means that those insuring agreements provide you with cover for Claims first made against you and notified to **Underwriters** during the **Policy Period**.

The policy does not provide cover in relation to Known Facts (as set out in the relevant exclusion) nor in relation to any actual or alleged act, error, omission or other conduct which takes place before the Retroactive Date (if any) specified in the schedule.

Where you give notice in writing to us of any facts that might give rise to a claim against you as soon as reasonably practicable after you become aware of those facts but before the expiry of the **Policy Period**, you may have rights under Section 40(3) of the Insurance Contracts Act 1984 to be indemnified in respect of any claim subsequently made against you arising from those facts notwithstanding that the **Claim** is made after the expiry of the **Policy Period**. Those rights arise under the legislation only. The terms of the policy and the effect of the policy is that you are not covered for Claims made against you after the expiry of the **Policy Period**.

Privacy Notice

LAUW and **Underwriters** are committed to compliance with the provisions of the Australian Privacy Principles and the Privacy Act 1988 (Commonwealth). In order for **Underwriters** to assess the risk of and provide you with insurance products and assess and manage any claims under those products, it is necessary to obtain personal information from you. If you do not provide us with this information, this may prevent **Underwriters** from providing you with the products or services sought.

If you provide us with information about someone else, you must obtain their consent to do so.

LAUW and **Underwriters** may disclose your information to other insurers, their reinsurers, and insurance reference service or other advisers used by **Underwriters** or LAUW on behalf of **Underwriters** such as loss adjusters, lawyers or others who may be engaged to assist in claims handling, underwriting or for the purpose of fulfilling compliance and/or regulatory requirements. These third parties will all be contractually required to adhere to **Underwriters**' privacy obligations.

Our privacy policy contains information about how you can access the information we hold about you, ask us to correct and how you may make a privacy related complaint. For further details please see: <http://lauw.com.au/privacy-policy.php>

We also supply your information to the providers of our policy administration and underwriting systems that help us to provide our products and services to you.

The above notes are not exhaustive and in no way should be read in isolation of the full policy terms, conditions, limitations and exclusions.

General Information

1.

Name of Company (Insured):

Address of registered or principal office:

Date of establishment:

2.

Please provide a full description of your business activities and detail if there are any anticipated changes to the activities in the next 12 months:

3.

Website:

Section A: Professional Indemnity Insurance

1.

If the company has been established for less than 3 years, can you confirm that one or more of the Directors has at least 3 years' experience in the relevant industry?

Yes No *Please attach CV's of Directors

2.

Please confirm your total number of employees:

3.

Is the company authorised and regulated by any corporate regulator?

Yes No If YES, please name the regulator

4.

Please provide annual financial details for the past year, current year and the projected income for the next financial year.

	Currency	Past Year	Current Year	Next year
Fee Income/Turnover				
Total Assets				
Profit Before Tax				

*Please provide a copy of latest report and accounts

5.

Please confirm geographical split of fee income/turnover by client / customer base:

	Past Year	Current Year	Next Year
Australia/New Zealand	%	%	%
USA	%	%	%
Rest of the World	%	%	%
	100 %	100 %	100 %

If you have entered a Rest of the World number, please list applicable countries below:

6.

Do you use a standard form of contract, agreement or letter of appointment with regard to services performed?

Yes No

Please provide a copy of your standard form of contract, agreement or letter of appointment.

7.

If you engage in business to business (B2B) contracts then please answer questions (a) and (b):

(a) Please list the five largest contracts undertaken during the last 3 years:

Client	Industry	Nature of your product or service	Fee	Start date	End date

(b) Do your standard delivery / contract terms:

- (i) accept liability for consequential or indirect losses?
 Yes No
- (ii) accept liability for financial damages greater than the value of contract?
 Yes No
- (iii) include any form of liquidated damages?
 Yes No
- (iv) warrant a performance standard greater than reasonable care and skill?
 Yes No
- (v) provide for an unlimited warranty period?
 Yes No
- (vi) allow for changes to the scope of work without a written variation of contract?
 Yes No
- (vii) provide indemnities to your clients (other than for liability for intellectual property rights, death, bodily injury, and/or property damage)?
 Yes No

If YES to any of the above, please provide more details below:

8.

If you engage in business to consumer (B2C) contracts then please answer questions (a) and (b):

(a) What is the largest value per transaction during the last 12 months?

--

(b) What is the average value per transaction during the last 12 months?

--

9.

(a) Do you seek legal advice relating to intellectual property protection and breaches prior to the release of any new products or technology?

Yes No

(b) Have you registered the intellectual property rights for your products and technology?

Yes No

(c) If you use third party owned intellectual property, do you obtain appropriate licenses and indemnifications?

Yes No

If NO to any of the above, please detail below what alternative controls are in place with regard to the management of intellectual property rights:

10.

Do you maintain an independent annual audit of your business functions including IT?

Yes No

11.

Are all publications and online material issued by the company reviewed by an in-house legal department and/or outside legal advisers?

Yes No

Section B: Directors & Officers Liability Insurance

If you require coverage for D&O please complete the following questions.

1.

Can you confirm that the company and all of its subsidiaries:

(a) Are registered in Australia?

Yes No

(b) Are not listed on any stock exchange or any other form of securities market?

Yes No

(c) Are not contemplating a share offering or rights issue in the next 12 months?

Yes No

(d) Have not sold any part of the company in the last 12 months?

Yes No

(e) Do not anticipate making any acquisitions or disposals in the next 12 months?

Yes No

(f) Have not had any directors leave the company in the last 12 months?

Yes No

(g) Do not have outside board positions that require coverage under this policy?

Yes No

(h) Do not have any shareholders that own 5% or more of the company that are not directors?

Yes No

If you have answered No to any of the questions above, please give details here:

Section C: Theft Insurance

If you require coverage for Theft please complete the following questions.

1.

Can you confirm that no more than \$10,000 in cash is held at the company's premises at any one time?

Yes No

2.

Are the duties of each employee arranged so that no one employee is permitted to control any transaction/process from start to finish?

Yes No

3.

Is there segregation of duties between those responsible for bank reconciliation and deposits, cheque signing and payroll?

Yes No

4.

Are background checks performed on all new employees?

Yes No

5.

Are company bank accounts reconciled weekly?

Yes No

6.

Are all passwords securely changed when staff leave?

Yes No

7.

Is the use of IT terminals restricted only to authorised personnel?

Yes No

8.

Are remote IT terminals kept in a physically secure location accessible to authorised personnel only?

Yes No

If you have answered No to any of the questions above, please give details here:

9.

Please provide details on the risk management procedures for avoiding and mitigating fraud/theft against the company and its customers (eg encryption, passwords, testing and other message authentication, call back, contractual disclaimers).

Please provide a copy of your procedures manual.

10.

Can you confirm the company adheres to the following best practices and minimum security standards?

(a) All electronic payments and sensitive data (including bank/credit card details) are encrypted?

Yes No

(b) Payments to customers are only made to verified customer bank accounts as recorded on the company's systems?

Yes No

(c) Prior to amending personal details (including bank account details) in your records, secondary confirmation is obtained from customers via a source different from the original communication and evidential proof of such changes is obtained?

Yes No

- (d) Customers can only access their accounts on your systems via a password?
 Yes No
- (e) You use anti-virus, anti-spyware and anti-malware software and update them regularly?
 Yes No
- (f) You use firewalls and other security applications between the internet and sensitive data?
 Yes No
- (g) You use intrusion detection or intrusion prevention systems (IDS/IPS) and these are monitored?
 Yes No

If NO to any of the above, please detail below along with mitigating comments

Section D: Cyber Insurance

If you require coverage for cyber please complete the following questions.

1.

(a) How many personally identifiable information (PII) records or unique consumer records does the company currently hold (including employees)?

- (b) Does the company hold or process any of the following types of sensitive data?
- | | |
|---|--|
| <input type="checkbox"/> Financial information (including credit/debit card records) | <input type="checkbox"/> Medical information |
| <input type="checkbox"/> Identity information (including NI number or passport details) | <input type="checkbox"/> Names, addresses, telephone numbers |

- 2.**
- Can you confirm the company adheres to the following best practices and minimum security standards?
- a) Have a dedicated individual responsible for Information Security and Privacy
 Yes No
 - b) Have a written incident management response plan
 Yes No
 - c) Does your Incident Response Plan reference mitigation steps for business continuity and recovery should a ransomware incident occur?
 Yes No
 - d) Perform background checks on all employees and contractors with access to sensitive data
 Yes No
 - e) Have restricted access to sensitive data (including physical records)
 Yes No
 - f) Have a process to delete systems access within 48 hours after employee termination
 Yes No
 - g) Have written information security policies and procedures that are reviewed annually and communicated to all employees including information security awareness training?
 Yes No
 - h) Ensure all remote access to IT systems is secure
 Yes No
 - i) Only use operating systems that continue to be supported by the original provider
 Yes No
 - j) You use anti-virus, anti-spyware and anti-malware software and update them regularly
 Yes No
 - k) You use firewalls and other security appliances between the Internet and sensitive data
 Yes No

l) You use intrusion detection or intrusion prevention systems (IDS/IPS) and these are monitored

Yes No

m) Do you train end users against phishing and social engineering threats via ongoing campaigns and assessments?

Yes No

n) You ensure all sensitive data on your system is encrypted

Yes No

o) Do you enforce a BYOD (Bring Your Own Device) policy that ensures critical data is encrypted when transferred to portable media devices (USBs, Laptops etc.)?

Yes No

p) You ensure all sensitive data on all removable media is encrypted

Yes No

q) You ensure sensitive data is permanently removed (e.g. physical destruction not merely deleting) from hard drives and other storage media and from paper records prior to disposal

Yes No

3.

1. Do you authenticate emails using:

SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and/or DMARC (Domain-Based Message Authentication)?

2. Do you use O365 in your organisation?

Yes. Have the following been implemented: MFA (multi factor authentication), ATP (advanced threat protection),

Macros disabled by default

No. Which product do you use for email monitoring (e.g. Proofpoint):

3. Do you allow local admin rights on workstations?

Yes No

4. Do administrative/privileged accounts use a privilege access management (PAM) tool (e.g. CyberArk)?

Yes No. Which product(s) do you use?

5. Do you use an endpoint protection (EPP) product?

Yes. If so, which product(s)

No

6. Have you deployed an endpoint detection and response (EDR) tool that covers 100% of:

Servers and Endpoint? If so:

Which product(s):

If the EDR tool offers AI/automated rules based enforcement, has this been enabled?

Yes No N/A

7. Does all remote access to your network and corporate email require multifactor authentication (MFA)?

Yes No

8. Have you disabled remote desktop protocol (RDP)?

Yes No

If No, have you implemented the following?

VPN MFA RDP Honeypots

9. Do you operate a SIEM (Security information and event management) monitored 24/7/365 by an internal SOC (Security Operations Center) or MSSP (managed security service provide)?

Yes No

10. Does your incident response plan (IRP) specifically address ransomware scenarios?

Yes No

11. How frequently do you back up critical data?

Daily Weekly Monthly Other, please explain below

12. Do you keep a copy of your critical backups offline and inaccessible from your network?

Yes No

13. Which of the following are used to store backups?

Cloud Secondary data centre Offline Within a separate network segment

14. Have the following been implemented to secure the backup environment?

Segmentation Encryption MFA Vaulted Credentials

15. Do you use any commercial backup solutions (e.g. Commvault)?

Yes No. Which product(s) do you use

16. Does your backup strategy include the use of immutable technologies?

Yes No

17. Is the integrity of these backups and your recovery plans regularly tested?

Yes No

If NO to any of the above, please detail below along with mitigating comments:

Please outline any additional controls your organisation has in place to mitigate the threat of ransomware attacks (e.g. tagging of external emails, DNS, network segmentation, vulnerability scanning, phishing training):

4.

(a) Do you have a disaster recovery plan (DRP) and/or business continuity plan (BCP) in place?

Yes No

(b) In your DRP / BCP, how long would it take for you to be fully operational again following an incident?

(c) How often do you test your DRP / BCP?

5.

Please provide details of the vendors for the following services: (or check box if it is managed and operated in-house)

	Vendor	In-house
(a) Internet service provider		<input type="checkbox"/>
(b) Cloud / hosting / data centre provider		<input type="checkbox"/>
(c) Payment processing		<input type="checkbox"/>
(d) Data or information processing (such as marketing or payroll)		<input type="checkbox"/>
(e) Offsite archiving, backup and storage		<input type="checkbox"/>

Section E: Products, Pollution and Public Liability

If you require cover for General Liability please complete the following questions.

1.

Could the failure of your product or service result in:

The loss of life or bodily injury to a person

Yes No

Damage or destruction to any physical property

Yes No

If YES to any of the above, please detail below

2.

Do you manufacture or produce anything involving hazardous liquids, hazardous gases, or any other hazardous substances?

Yes No

If YES to the above, please detail below

3.

What proportion of your work is carried out at the following locations?

Your own premises	Client's premises	Public areas
%	%	%

4.

What proportion of your products have been sold continuously for:

Less than 1 year	1-3 years	Over 3 years
%	%	%

5.

Please detail your procedure for testing your products and quality assurance?:

Section F: Stamp Duty Split

For the purpose of calculating Stamp Duty please confirm the number of employees in the relevant State of Australia:

NSW	VIC	QLD	SA	WA	TAS	ACT	NT	Overseas

Section G: Claims History

1.

After having made full enquiries, including of all directors, partners and principals, can you confirm that:

(a) No claims (successful or otherwise) have been made against or have been threatened to made against:

(i) the company or any of its predecessors in respect to any negligence, breach of duty of care, infringement of any intellectual property right, libel or slander, dishonesty of any employee or to any other act, error or omission that that has or might have given rise to a claim?

Yes No

(ii) any director, partner or officer in respect to any wrongful act committed by them whilst acting in such capacity?

Yes No

(b) In the last 5 years the company or any director/employee has not been subject to any regulatory investigation?

Yes No

(c) The company has not suffered from any attempt, successful or otherwise:

(i) to steal any money, financial instruments or any other asset that it either owns or for which it is legally responsible.

Yes No

(ii) of extortion against it by a threat to commit a theft, cyber- attack or other malicious or criminal event.

Yes No

(d) The company has not received complaints, whether oral or in writing, regarding its services performed, products or solutions sold or provided, or advice given?

Yes No

(e) The company has not been adversely affected by or suffered any loss from any:

(i) privacy breach, virus, distributed denial of service (DDOS), telephone phreaking or hacking incident?

Yes No

(ii) unforeseen down time to its website or IT network of more than 3 hours?

Yes No

(f) You are not aware of any circumstance or problem that might in the future give rise to a claim against or a loss for the company or any of its directors, officers or partners that is covered under the proposed insurance policy?

Yes No

If NO to any of the above, please provide full details:

Section H: Insurance Details

1.

Quote Request

What limit of indemnity is required?	Do you buy this cover currently?
PI	<input type="checkbox"/> Yes <input type="checkbox"/> No
D&O	<input type="checkbox"/> Yes <input type="checkbox"/> No
Theft	<input type="checkbox"/> Yes <input type="checkbox"/> No
Cyber	<input type="checkbox"/> Yes <input type="checkbox"/> No
General Liability	<input type="checkbox"/> Yes <input type="checkbox"/> No

Declaration

I/We declare that the above answers, statements, particulars and additional information are true to the very best of our knowledge and belief. After full enquiry, I/We also confirm that I/We have disclosed all information and material facts that may alter the Underwriters' view of the risk, or affect their assessment of the exposures they are covering under the policy. I/We understand that all answers, statements, particulars and additional information supplied with this proposal form will become part of and form the basis of the policy.

I/We acknowledge that we have read and understood the content of the Important Notices contained in this proposal.

Signed:



Date:

Position:

For and/on behalf of the Proposer:

Name in capital letters (printed):

*the signatory should be a director or senior officer of, or a partner of, the company.