

SAN FRANCISCO

▶ LONDON

▶ LOS ANGELES

▶ PHILADELPHIA



evo 3.0

OUR EVOLVED CYBER POLICY

750 BATTERY STREET, 7TH FLOOR, SAN FRANCISCO, CA 941 11

WWW.EVOLVEMGA.COM



PREAMBLE

This Policy is a contract of insurance between **you** and **us**. **Your** Policy contains all the details of the cover that **we** provide. This Policy consists of and must be read together with the Declarations page and any Clauses and Endorsements that are attached to this Policy. This Policy is not complete unless it is signed and a Declarations page is attached.

The Sections of this Policy are identified by the blue lines across the page with upper case print, these are for information purposes only and do not form part of the cover given by this Policy. Terms in bold upper case print are references to specific Insuring Clauses, Sections or Conditions. Other terms in bold lower case print are defined terms and have a special meaning as set forth in the Definitions section and elsewhere. Words stated in the singular will include the plural and vice versa.

In consideration of the **premium** and in reliance upon the information that **you** provided to **us** prior to the commencement of this insurance, **we** agree to provide the cover as set out below.

INSURING CLAUSES

INSURING CLAUSE 1: CYBER INCIDENT RESPONSE

SECTION A: INCIDENT RESPONSE COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

- a. gain access to **our** 24/7 cyber incident response hotline;
- b. engage with **our cyber incident manager** who will coordinate the initial response;
- c. obtain initial advice and consultancy from **our cyber incident manager**, including threat intelligence in relation to the **cyber event**; and
- d. obtain initial remote support and assistance from **our cyber incident manager** to respond to the **cyber event**.

SECTION B: LEGAL AND REGULATORY COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred as a direct result of a **cyber event** which is first discovered by **you** during the **period of the policy** to:

- a. obtain legal advice to determine the correct course of action;
- b. draft **privacy breach** notification letters, substitute notices, website notices or e-mail notification templates;
- c. notify any appropriate governmental, regulatory, law enforcement, professional or statutory body;

- d. respond to any **regulatory investigation**; and
- e. defend any regulatory action.

SECTION C: IT SECURITY AND FORENSIC COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

- a. engage with an external IT security consultant to identify the source and scope of the **cyber event**;
- b. obtain initial advice to remediate the impact of the **cyber event**;
- c. conduct a forensic investigation of **your computer systems** where reasonable and necessary or as required by law or a regulatory body (including a requirement for a PCI Forensic Investigator);
- d. contain and remove any malware discovered on **your computer systems**; and
- e. engage with an IT security consultant to provide expert witness testimony at any trial or hearing arising from the **cyber event**.

SECTION D: CRISIS COMMUNICATION COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

- a. engage with a crisis communications consultant to obtain specific advice in direct relation to the **cyber event**;
- b. coordinate media relations in response to the **cyber event**;
- c. receive training for relevant spokespeople with respect to media communications in direct relation to the **cyber event**; and
- d. formulate a crisis communications plan in order to reduce damage to **your** brand and reputation as a direct result of the **cyber event**.

SECTION E: PRIVACY BREACH MANAGEMENT COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred as a direct result of a **cyber event** first discovered during the **period of the policy** to:

- a. print and post appropriate notices for any individual affected by the actual or suspected **cyber event** or to send e-mail notices or issue substitute notices;
- b. provide credit monitoring services, identity monitoring services, identity restoration services or identity theft insurance to affected individuals;
- c. set up a call center to manage inbound and outbound calls in direct relation to the **cyber event**; and
- d. provide translation services to manage communications with affected individuals.

SECTION F: THIRD PARTY PRIVACY BREACH MANAGEMENT COSTS

We agree to pay on behalf of any **third party** any reasonable sums necessarily incurred as a direct result of a **cyber event** first discovered during the **period of the policy** to:

- a. print and post appropriate notices for any individual affected by the actual or suspected **cyber event** or to send e-mail notices or issue substitute notices;
- b. provide credit monitoring services, identity monitoring services, identity restoration services or identity theft insurance to affected individuals;
- c. set up a call center to manage inbound and outbound calls in direct relation to the **cyber event**; and
- d. provide translation services to manage communications with affected individuals;

provided that **you** have contractually indemnified the **third party** against this **cyber event** and they have a legal obligation to notify affected individuals.

SECTION G: POST BREACH REMEDIATION COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred with **our cyber incident manager** following a **cyber event** covered under **INSURING CLAUSE 1 (SECTIONS A, B, C, D, E and F only)** for the following services in order to mitigate the potential of a future **cyber event**:

- a. complete an information security risk assessment;
- b. conduct an information security gap analysis;
- c. develop an information security document set; and
- d. deliver an information security awareness training session.

INSURING CLAUSE 2: CYBER CRIME

SECTION A: FUNDS TRANSFER FRAUD

We agree to reimburse **you** for **loss** first discovered by **you** during the **period of the policy** as a direct result of any **third party** committing:

- a. any unauthorized electronic funds transfer;
- b. theft of money or other financial assets from **your** bank by electronic means;
- c. theft of money or other financial assets from **your** corporate credit cards by electronic means;
- d. any fraudulent manipulation of electronic documentation whilst stored on **your** computer systems; or
- e. any phishing, vishing or other social engineering attack against any **employee** or **senior executive officer** that results in the transfer of **your** funds to an unintended **third party**.

SECTION B: THEFT OF FUNDS HELD IN ESCROW

We agree to reimburse **you** for **loss** (including compensation **you** are required to pay) first discovered by **you** during the **period of the policy** as a direct result of **you** having to reimburse any **third party** for theft, committed by a **third party** by electronic means, of their money or other financial assets from a bank account held by **you** on their behalf.

SECTION C: THEFT OF PERSONAL FUNDS

We agree to reimburse any **senior executive officer** for personal financial **loss** first discovered by them during the

period of the policy as a direct result of any **third party** compromising the **company's** network security which results in:

- a. theft of money or other financial assets from a personal bank account of the **senior executive officer**; or
- b. identity theft of the **senior executive officer** as a result of a **privacy breach** suffered by **you**.

SECTION D: EXTORTION

We agree to reimburse **you** for any ransom paid in response to an extortion demand first discovered by **you** during the **period of the policy** as a direct result of any threat to:

- a. introduce malware, or the actual introduction of malware, including Ransomware, into **your computer systems**;
- b. prevent access to **your computer systems** or data or any **third party** systems hosting **your** applications or data, including **cloud computing providers**;
- c. reveal **your** confidential information or confidential information entrusted to **you**; or
- d. damage **your** brand or reputation by posting false or misleading comments about **you** on social media sites.

SECTION E: CORPORATE IDENTITY THEFT

We agree to reimburse **you** for **loss** first discovered by **you** during the **period of the policy** arising as a direct result of the fraudulent use or misuse of **your** electronic identity including the establishment of credit in **your** name, the electronic signing of any contract, the creation of any website designed to impersonate **you** or the reliance by any **third party** on a fraudulent version of **your** digital identity.

SECTION F: TELEPHONE HACKING

We agree to reimburse **you** for **loss** first discovered by **you** during the **period of the policy** as a direct result of **your** telephone system being hacked by a **third party** including the cost of unauthorized calls or unauthorized use of **your** bandwidth.

SECTION G: FRAUDULENT COMMUNICATIONS

We agree to reimburse **you** in the event of fraudulent electronic communications or websites designed to impersonate **you** or any of **your** products first discovered by **you** during the **period of the policy**, for:

- a. the cost of creating and issuing a specific press release or establishing a specific website to advise **your** customers and prospective customers of the fraudulent communications; and
- b. the cost of reimbursing **your** existing customers for their financial loss arising directly from the fraudulent communications; and
- c. **your direct loss of profits** for 90 days following **your** discovery of the fraudulent communications as a direct result of the fraudulent communications; and
- d. external costs associated with the removal of websites designed to impersonate **you**.

INSURING CLAUSE 3: SYSTEM DAMAGE AND BUSINESS INTERRUPTION

SECTION A: SYSTEM DAMAGE AND RECTIFICATION COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred to repair and restore the data and application components of **your computer systems** that have been damaged as a direct result of a **cyber event** first discovered by **you** during the **period of the policy**.

For the purposes of this Section **we** will only reimburse the following elements of **your** financial loss:

- a. the additional cost of employing contract staff or overtime costs for **employees** to rebuild **your** data, including the cost of data re-entry or data re-creation;
- b. the additional cost of employing specialist consultants, including IT forensic consultants, to recover **your** data or applications; and
- c. the additional cost of employing specialist consultants or overtime costs for **employees** working within **your** IT department to reconstitute **your computer systems** to the position they were in immediately prior to the **cyber event**.

SECTION B: SYSTEM BUSINESS INTERRUPTION

We agree to reimburse **you** for **your** financial loss sustained during the **indemnity period** as a direct result of a **system outage** first discovered by **you** during the **period of the policy**.

This financial loss will only be covered where the **system outage** is a direct result of a **cyber event** and the **system outage** lasts for longer than the **time retention**.

For the purposes of this Section **we** will only reimburse those elements of **your** financial loss that constitute **your direct loss of profits** and **additional expenditure** including the reasonable and necessary:

- a. additional costs of sourcing **your** products or services from alternative sources in order to meet contractual obligations to supply **your** customers;
- b. additional costs of employing contract staff or overtime costs for **employees** in order to continue **your business operations**;
- c. additional costs of employing specialist consultants, including IT forensic consultants to diagnose the source of the **system outage**; and
- d. overtime costs for **employees** working within **your** IT department to diagnose and fix the source of the **system outage**.

SECTION C: CONSEQUENTIAL REPUTATIONAL HARM

We agree to reimburse **you** for **your direct loss of profits** sustained during the **reputational harm period** as a direct result of the loss of current or future customers caused by damage to **your** reputation as a result of a **cyber event** first discovered by **you** during the **period of the policy**.

SECTION D: LOSS ADJUSTMENT COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred to determine the amount of **your** financial loss

following an interruption to **your business operations** covered under **INSURING CLAUSE 3 (SECTIONS A, B and C only)**. We will only pay these costs where they are incurred with an independent expert appointed by the **cyber incident manager**.

INSURING CLAUSE 4: NETWORK SECURITY & PRIVACY LIABILITY

SECTION A: NETWORK SECURITY LIABILITY

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including the establishment of any consumer redress fund and associated expenses) as a result of any **claim** arising out of a **cyber event** first discovered by **you** during the **period of the policy** that results in:

- a. the transmission of malware to a **third party's computer system**;
- b. **your computer systems** being used to carry out a denial of service attack;
- c. **your** failure to prevent unauthorized access to information stored or applications hosted on **your computer systems** or a **cloud computing provider's system**; and
- d. identity theft, experienced by **your employees, senior executive officers** or any **third party**.

We will also pay **costs and expenses** on **your** behalf.

SECTION B: PRIVACY LIABILITY

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including the establishment of any consumer redress fund and associated expenses) as a result of any **claim** arising out of a **cyber event** first discovered by **you** during the **period of the policy** that results in:

- a. an actual or suspected disclosure of or unauthorized access to any personally identifiable information (PII), including payment card information or protected healthcare information (PHI);
- b. **your** failure to adequately warn affected individuals of a **privacy breach**, including the failure to provide a data breach notification in a timely manner;
- c. a breach of any rights of confidentiality as a direct result of **your** failure to maintain the confidentiality of any data pertaining to an **employee** or a **senior executive officer**;
- d. a breach of any rights of confidentiality, including a breach of any provisions of a non-disclosure agreement or breach of a contractual warranty relating to the confidentiality of commercial information, PII, or PHI;
- e. a breach of any part of **your** privacy policy; or
- f. actual or suspected disclosure of or unauthorized access to **your** data or data for which **you** are responsible.

We will also pay **costs and expenses** on **your** behalf.

SECTION C: MANAGEMENT LIABILITY

We agree to pay on behalf of any **senior executive officer** all sums they become legally obliged to pay as a result of any **claim** made against them arising directly out of a **cyber event** first discovered by **you** during the **period of the policy**.

We will also pay **costs and expenses** on behalf of **your senior executive officers**.

However, **we** will not make any payment under this Section for which the **senior executive officer** is entitled to indemnity under any other insurance, except for any additional sum which is payable over and above the other insurance.

SECTION D: REGULATORY FINES

We agree to pay on **your** behalf any fines and penalties resulting from a **regulatory investigation** arising as a direct result of a **cyber event** first discovered by **you** during the **period of the policy**.

We will also pay **costs and expenses** on **your** behalf.

SECTION E: PCI FINES, PENALTIES AND ASSESSMENTS

We agree to pay on **your** behalf any fines, penalties and card brand assessments including fraud recoveries, operational reimbursements, non-cooperation costs and case management fees which **you** become legally obliged to pay **your** acquiring bank or payment processor as a direct result of a **payment card breach** first discovered by **you** during the **period of the policy**.

We will also pay **costs and expenses** on **your** behalf.

INSURING CLAUSE 5: MEDIA LIABILITY

SECTION A: DEFAMATION

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including liability for claimants' costs and expenses) as a result of any **claim** first made against **you** during the **period of the policy** for any:

- a. defamation, including but not limited to libel, slander, trade libel, product disparagement and injurious falsehood; or
- b. emotional distress or outrage based on harm to the character or reputation of any person or entity;

arising out of any **media content**.

We will also pay **costs and expenses** on **your** behalf.

SECTION B: INTELLECTUAL PROPERTY RIGHTS INFRINGEMENT

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including liability for claimants' costs and expenses) as a result of any **claim** first made against **you** during the **period of the policy** for any:

- a. infringement of any intellectual property rights, including, but not limited to, copyright, trademark, trade dilution, trade dress, commercial rights, design rights, domain name rights, image rights, moral rights, service mark or service name, but not including patent;
- b. act of passing-off, piracy or plagiarism or any misappropriation of content, concepts, format rights or ideas or breach of a contractual warranty relating to intellectual property rights;

- c. breach of any intellectual property rights license acquired by **you**; or
- d. failure to attribute authorship or provide credit;

arising out of any **media content**.

We will also pay **costs and expenses** on **your** behalf.

INSURING CLAUSE 6: TECHNOLOGY ERRORS AND OMISSIONS

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including liability for claimants' **costs and expenses**) as a result of any **claim** first made against **you** during the **period of the policy** arising out of any act, error, omission or breach of contract in the provision of **your technology services**.

We will also pay **costs and expenses** on **your** behalf.

INSURING CLAUSE 7: COURT ATTENDANCE COSTS

We agree to reimburse **you** for any reasonable sums necessarily incurred by **you** with **our** prior written agreement (which will not be unreasonably withheld) to attend court or any tribunal, arbitration, adjudication, mediation or other hearing in connection with any claim for which **you** are entitled to indemnity under this Policy.

HOW MUCH WE WILL PAY

YOUR MAXIMUM LIMITS UNDER THIS POLICY

The maximum amount payable by **us** under this Policy for any one claim or series of related claims is the **policy limit** plus the **incident response limit**.

The maximum amount payable by **us** under any Insuring Clause for any one claim or series of related claims is the amount shown as the limit in the Declarations page for that Insuring Clause.

The maximum amount payable by **us** under any Section for any one claim or series of related claims is the amount shown as the limit in the Declarations page for that Section.

YOUR MAXIMUM LIMIT FOR RELATED INCIDENTS

Where more than one claim arises from the same original cause or single source or event, all of those claims will be deemed to be one claim and only one **policy limit** and one **incident response limit** will apply in respect of that claim.

In the event that cover is provided under multiple Insuring Clauses or multiple Sections for any one claim, only one **policy limit** and one **incident response limit** will apply in total for that claim.

YOUR AGGREGATE LIMIT FOR LIABILITY CLAIMS

In respect of **INSURING CLAUSES 4, 5, 6 and 7**, the maximum amount payable under this Policy in total aggregate will be the **policy limit**.

In respect of **INSURING CLAUSES 4, 5, 6 and 7**, we may at any time pay to **you** in connection with any **claim** the amount of the **policy limit** (after deduction of any amounts already paid). Upon that payment being made **we** will relinquish the conduct and control of the **claim** and be under no further liability in connection with that **claim** except for the payment of **costs and expenses** incurred prior to the date of such payment (unless the **policy limit** is stated to be inclusive of **costs and expenses**).

If **costs and expenses** are stated in the Declarations page to be in addition to the **policy limit** plus the **incident response limit**, or if the operation of local laws require **costs and expenses** to be paid in addition to the **policy limit** plus the **incident response limit**, and if a damages payment in excess of the **policy limit** plus the **incident response limit** has to be made to dispose of any **claim**, our liability for **costs and expenses** will be in the same proportion as the **policy limit** plus the **incident response limit** bears to the total amount of the damages payment.

YOUR DEDUCTIBLE

We will only be liable for that part of each and every claim which exceeds the amount of the **deductible**. If any expenditure is incurred by **us** which falls within the amount of the **deductible**, then **you** will reimburse that amount to **us** upon **our** request.

Where more than one claim arises from the same original cause or single source or event all of those claims will be deemed to be one claim and only one **deductible** will apply.

In respect of **INSURING CLAUSE 3 (SECTION B only)**, a single **time retention, deductible** and **indemnity period** will apply to each **claim**. Where the same original cause or single source or event causes a series of system outages these will be considered one **system outage** whose total duration is equal to the cumulative duration of each individual outage.

Where cover is provided under multiple Sections or multiple Insuring Clauses only one **deductible** will apply to that claim and this will be the highest **deductible** of the Sections under which cover is provided.

DEFINITIONS

1. **“Additional expenditure”** means costs incurred by **you** as a direct result of the complete or partial failure of **your business operations** over and above **your** normal operating expenses where these costs are designed to minimize **your direct loss of profits** and maintain continuity of **your business operations**, subject to the costs incurred being less than the potential **direct loss of profits** during the **indemnity period** had the costs not been incurred.

2. **“Approved claims panel providers”** means the approved claims panel providers stated in the declarations page.

3. **“Business operations”** means the business operations stated in the Declarations page.

4. **“Claim”** means
 - a. a written demand for compensation;
 - b. a written request for a retraction or a correction;
 - c. a threat or initiation of a lawsuit; or
 - d. a disciplinary action or **regulatory investigation**.

made against **you**.

5. **“Client”** means any **third party** with whom **you** have a contract in place for the supply of **your** business services in return for a fee, or where a fee would normally be expected to be paid.

6. **“Cloud computing provider”** means a **third party** that provides **you** with hosted computing services accessed across the internet or dedicated network links including infrastructure, platform, file storage and application level services.

7. **“Company”** means the company named as the Insured in the Declarations page or any **subsidiary**.

8. **“Computer systems”** means all electronic computers including operating systems, software, hardware and all communication and open system networks and any data or websites wheresoever hosted, including cloud computing providers, off-line media libraries and data back-ups and mobile devices including but not limited to smartphones, iPhones, tablets or personal digital assistants.

9. **“Continuity date”** means
the first date upon which cover was inceptioned with **us** as stated as the continuity date in the Declarations page.
10. **“Costs and expenses”** means
- a. **third party** legal and professional expenses (including disbursements) reasonably incurred in the defense of **claims** or circumstances which could reasonably be expected to give rise to a **claim** or in quashing or challenging the scope of any injunction, subpoena or witness summons;
 - b. any post judgment interest; and
 - c. the cost of appeal, attachment and similar bonds including bail and penal bonds.
- Subject to all **costs and expenses** being incurred with the **cyber incident manager’s** prior written agreement.
11. **“Cyber Event”** means
any actual or suspected unauthorized system access, electronic attack or **privacy breach**, including denial of service attack, cyber terrorism, hacking attack, Trojan horse, phishing attack, man-in-the-middle attack, application-layer attack, compromised key attack, malware infection (including spyware or Ransomware) or computer virus.
12. **“Cyber incident manager”** means
the company or individual named as the cyber incident manager in the Declarations page.
13. **“Cyber incident response line”** means
the telephone number stated as the cyber incident response line in the Declarations page.
14. **“Deductible”** means
the amount stated as the deductible in the Declarations page.
15. **“Direct loss of profits”** means
your income that, had the **cyber event** not occurred, would have been generated directly from **your business operations** (less sales tax) during the **indemnity period**, less:
- a. actual income (less sales tax) generated directly from **your business operations** during the **indemnity period**; and
 - b. any cost savings achieved as a direct result of the reduction in income.
16. **“Employee”** means
any employee, volunteer or contract employee of the **company**, other than a **senior executive officer**.
17. **“Expiry date”** means
the expiry date stated in the Declarations page.
18. **“Inception date”** means
the inception date stated in the Declarations page.

17. **"Incident response limit"** means
the highest individual limit available where cover is applicable under **INSURING CLAUSE 1** as stated in the Declarations page.
20. **"Indemnity period"** means
the period starting from the first occurrence of a **system outage** and lasting for the period stated as the indemnity period in the Declarations page.
21. **"Loss"** means
any direct financial loss sustained by the **company**.
22. **"Media content"** means
any content created or disseminated by **you** or on **your** behalf, including but not limited to content disseminated through books, magazines, brochures, social media, billboards, websites, mobile applications, television and radio.
- "Media content"** does not include any:
- a. tangible product design;
 - b. industrial design;
 - c. architectural or building services;
 - d. any advertisement created by **you** for a **third party**;
 - e. business, company, product or trading name;
 - f. product packaging or labeling; or
 - g. software products.
23. **"Payment card breach"** means
an actual or suspected unauthorized disclosure of payment card data stored or processed by **you** arising out of an electronic attack, accidental disclosure or the deliberate actions of a rogue **employee**.
- "Payment card breach" does not mean a situation where payment card data is deliberately shared with or sold to a **third party** with the knowledge and consent of a **senior executive officer**.
24. **"Period of the policy"** means
the period between the **inception date** and the **expiry date** or until the Policy is canceled in accordance with **CONDITION 4**.
25. **"Policy limit"** means
the highest individual limit available where cover is applicable under any Insuring Clause or Section as stated in the Declarations page.
26. **"Premium"** means
the amount stated as the premium in the Declarations page and any subsequent adjustments.

26. **"Privacy breach"** means
an actual or suspected unauthorized disclosure of information arising out of an electronic attack, accidental disclosure or the deliberate actions of a rogue **employee**.
- "Privacy breach"** does not mean a situation where information is deliberately shared with or sold to a **third party** with the knowledge and consent of a **senior executive officer**.
28. **"Regulatory investigation"** means
a formal hearing, official investigation, examination, inquiry, legal action or any other similar proceeding initiated by a governmental, regulatory, law enforcement, professional or statutory body against **you**.
29. **"Reputational harm period"** means
the period starting from when the **cyber event** is first discovered and lasting for the period stated as the reputational harm period in the Declarations page.
30. **"Senior executive officer"** means
board members, C-level executives, in-house lawyers and risk managers of the **company**.
31. **"Subsidiary"** means
any entity of which the company stated as the insured in the Declarations page has majority ownership on or before the **inception date**.
32. **"System outage"** means
a degradation in the performance of **your computer systems** which renders them incapable of supporting their normal business function.
33. **"Technology services"** means
the supply by **you** of technology services to **your client**, including but not limited to hardware, software, data processing, internet services, data and application hosting, computer systems analysis, consulting, training, programming, installation, integration, support and network management.
34. **"Third party"** means
any person who is not an **employee** or any legal entity that is not the **company**.
35. **"Time retention"** means
the number of hours stated as the time retention in the Declarations page.
36. **"We/our/us"** means
the underwriters stated in the Declarations page.

32. "You/your" means

the **company**, **employees** and **senior executive officers** solely acting in the normal course of **your business operations**.

EXCLUSIONS

We will not make any payment under this Policy:

EXCLUSIONS RELATING TO SYSTEM DAMAGE AND BUSINESS INTERRUPTION

In respect of **INSURING CLAUSE 3** only:

1. **Business interruption liability**

for that part of any **claim** that constitutes actual or alleged liability to a **third party**, or legal costs in the defense of any **claim**, including customer compensation.

EXCLUSIONS RELATING TO ALL INSURING CLAUSES

2. **Antitrust**

In respect of **INSURING CLAUSES 5** and **6**, for or arising out of any actual or alleged antitrust violation, restraint of trade, unfair competition, false, deceptive or unfair trade practices, violation of consumer protection laws or false or deceptive advertising.

3. **Associated Companies**

- a. in respect of any **claim** made by any company, firm or partnership in which the **company** has greater than a 10% executive or financial interest, unless the **claim** emanates from an independent **third party**;
- b. in respect of any **claim** made by any company, firm, partnership or individual which has greater than a 10% executive or financial interest in the **company**, unless the **claim** emanates from an independent **third party**;
- c. arising out of or resulting from any of **your** activities as a trustee, partner, officer, director or employee of any employee trust, charitable organization, corporation, company or business other than that of the **company**;
or
- d. in respect of any **claim** made by or on behalf of the **company** against a **third party**

4. **Betterment**

which results in **you** being in a better financial position or **you** benefitting from upgraded versions of **your computer systems** as a direct result of the event which gave rise to the claim under this policy.

However, in the event of a hacking attack, malware infection or computer virus, when rebuilding **your computer systems** we will pay the additional costs and expenses incurred to install a more secure and efficient version of the affected **computer system**, provided that the maximum amount we will pay is 25% more than the cost that would have been incurred to repair or replace the original model or license. Under no circumstances will we pay the cost of acquiring or installing **computer systems** which did not form a part of **your computer systems** immediately prior to the incident which gave rise to the claim.

This Exclusion will not apply to **INSURING CLAUSE 1 (SECTION G only)**.

5. Chargebacks

for any credit card company or bank, wholly or partially, reversing or preventing a payment transaction, unless specifically covered under **INSURING CLAUSE 4 (SECTION E only)** for which **you** have purchased coverage.

6. Core internet infrastructure failure

arising directly from a failure, material degradation or termination of any core element of the internet, telecommunications or GPS infrastructure that results in a regional, countrywide or global outage of the internet, including a failure of the core DNS root servers, satellite network or the IP addressing system or an individual state or non-state actor turning off all or part of the internet.

7. Domain name suspension or revocation

arising directly or indirectly from the suspension, cancellation, revocation or failure to renew any of **your** domain names or uniform resource locators.

8. Insolvency

arising out of or relating directly or indirectly to **your** insolvency or bankruptcy, or the insolvency or bankruptcy of any **third party**. However, **your** insolvency will not relieve **us** of any of **our** legal obligations under this contract of insurance where this insolvency does not give rise to a **claim** under this Policy.

9. Known claims and circumstances

arising out of any actual or suspected **cyber event, claim** or circumstance which might give rise to a **claim** which a **senior executive officer** was aware of, or ought reasonably to have been aware of, prior to the **continuity date**, including any claim or circumstance notified to any other insurer.

10. Liquidated damages, service credits and penalty clauses clauses

for liquidated damages or service credits, or arising out of penalty clauses unless **you** would have been liable in the absence of any contract stipulating the liquidated damages or service credits or penalty clauses.

11. Loss of economic value

for the reduction in economic or market value (including **loss** of potential future sales) of any of **your** intellectual property assets.

12. Management liability

for any sums that **your senior executive officers** become legally obliged to pay, including **costs and expenses**, as a result of any **claim** made against them arising out of a **cyber event**.

However, this Exclusion will not apply to **INSURING CLAUSE 4 (SECTION C only)**.

13. Misleading advertising

arising directly or indirectly from any advertisement, promotion or product description that is actually or alleged to be false or misleading.

14. Nuclear

arising directly or indirectly from or contributed to by:

- a. ionising radiations or contamination by radioactivity from any nuclear fuel or from any nuclear waste from the combustion of nuclear fuel; or
- b. the radioactive, toxic, explosive or other hazardous properties of any explosive nuclear assembly or nuclear component.

15. Patent infringement

arising directly or indirectly out of the actual or alleged infringement of any patent or inducing the infringement of any patent.

16. Payment card industry related fines, penalties and assessments

for fines, penalties and card brand assessments, including fraud recoveries, operational reimbursements, non-cooperation costs and case management fees which **you** become legally obliged to pay **your** acquiring bank or payment processor as a direct result of a **payment card breach**.

However, this Exclusion will not apply to **INSURING CLAUSE 4 (SECTION E only)**.

17. Power failure

arising directly or indirectly from any failure in the power supply, including that caused by any surge or spike in voltage, electrical current or transferred energy.

18. Product IP infringement

arising directly or indirectly from the actual or alleged infringement of any intellectual property right by any product manufactured, designed, formulated, licensed, distributed, or sold by **you** or the misappropriation of any trade secret by **you** or a **third party**.

19. Professional liability

arising directly out of any negligent advice or professional services provided to a **client** for a fee except when arising directly from a **cyber event**.

However, this Exclusion will not apply to **INSURING CLAUSE 6**.

20. Property and hardware costs

for any tangible property repair or replacement including the cost of repairing any hardware or replacing any tangible property or equipment that forms part of **your computer systems**.

However, where repairing or replacing hardware or tangible property or equipment is a more practical and cost effective solution than installing new firmware onto **your** existing components, **we** will pay the **costs and expenses** required to do so.

21. Regular hours staff costs

for normal salary and bonus costs paid to **employees** or **senior executive officers** working their regular, contracted hours.

22. Sanctions

to the extent that the provision of such cover or payment will expose **us** to any sanction, prohibition or restriction under the United Nations resolutions or the trade or economic sanctions, laws or regulations of Australia, Canada, the European Union, United Kingdom or United States of America.

23. Theft of funds in escrow

for theft of money or other financial assets belonging to a **third party**.

However, this Exclusion will not apply to **INSURING CLAUSE 2 (SECTION B)** only).

24. Uninsurable fines

for fines, penalties, civil or criminal sanctions, and for multiple, punitive or exemplary damages, unless insurable by law.

25. Unlawful surveillance

in respect of any actual or alleged eavesdropping, wiretapping, or unauthorized audio or video recording committed by **you** or by a **third party** on **your** behalf with the knowledge and consent of **your senior executive officers**.

26. Unsolicited communications

arising directly or indirectly from any actual or alleged violation of:

- a. the CAN-SPAM Act of 2003 or any subsequent amendments to that Act;
- b. the Telephone Consumer Protection Act (TCPA) of 1991 or any subsequent amendments to that Act;
or
- c. any other law, regulation or statute relating to unsolicited communication, distribution, sending or transmitting of any communication via telephone or any other electronic or telecommunications device.

27. War and terrorism

arising directly or indirectly out of:

- a. war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not), civil war, rebellion, insurrection, civil commotion assuming the proportions of or mounting to an uprising, military or usurped power; or
- b. any act or threat of force or violence by an individual or group, whether acting alone or on behalf of or in connection with any organization or government, committed for political, religious, ideological or similar purposes including the intention to influence any government or to put the public, or any section of the public, in fear; and
- c. any action taken in controlling, preventing, suppressing or in any way relating to a. or b. above.

However, this Exclusion does not apply to a **cyber event** affecting **your computer systems** or a **cloud computing provider's** systems.

28. Willful or dishonest acts of senior executive officers

arising directly or indirectly out of any willful, criminal, malicious or dishonest act, error or omission by a **senior executive officer** as determined by final adjudication, arbitral tribunal or written admission.

CONDITIONS

1. What you must do if an incident takes place

If any **senior executive officer** becomes aware of any incident which may reasonably be expected to give rise to a claim under this Policy, **you** must:

- a. other than in accordance with **CONDITION 2**, notify the **cyber incident manager** as soon as is reasonably practicable and follow their directions. However, this notification must be made no later than the end of any applicable extended reporting period. A telephone call to **our cyber incident response line** or confirmed notification via our cyber incident response app will constitute notification to the **cyber incident manager**; and
- b. in respect of **INSURING CLAUSES 4, 5 and 6**, not admit liability for or settle or make or promise any payment or incur any **costs and expenses** without **our** prior written agreement (which will not be unreasonably withheld).

Due to the nature of the coverage offered by this Policy, any unreasonable delay by **you** in notifying the **cyber incident manager** could lead to the size of the claim increasing or to **our** rights of recovery being restricted. **We** will not be liable for that portion of any claim that is due to any unreasonable delay in **you** notifying the **cyber incident manager** of any incident in accordance with this clause. However, if **you** are prevented from notifying **us** by a legal or regulatory obligation then **your** rights under this Policy will not be affected.

If **you** discover a **cyber event** **you** may only incur costs without **our** prior written consent within the first 72 hours following the discovery and any **third party** costs incurred must be with a company forming part of the **approved claims panel providers**. All other costs may only be incurred with the prior written consent of the **cyber incident manager** (which will not be unreasonably withheld).

2. What you must do in the event of a circumstance which could give rise to a claim

In respect of **INSURING CLAUSES 5** and **6**, should a **senior executive officer** become aware of:

- a. a situation during the **period of the policy** that could give rise to a **claim**; or
- b. an allegation or complaint made or intimated against **you** during the **period of the policy**;

then **you** have the option of whether to report this circumstance to **us** or not. However, if **you** choose not to report it this circumstance **we** will not be liable for that portion of any **claim** that is greater than it would have been had **you** reported this circumstance.

If **you** choose to report this circumstance **you** must do so no later than the end of any applicable extended reporting period for it to be considered under this Policy and **we** will require **you** to provide full details of the circumstance, including but not limited to:

- a. the time, place and nature of the circumstance;
- b. the manner in which **you** first became aware of this circumstance;
- c. the reasons why **you** believe that this circumstance could give rise to a **claim**;
- d. the identity of the potential claimant; and
- e. an indication as to the size of the **claim** that could result from this circumstance.

Any subsequent **claim** arising directly from this circumstance will be deemed to have been made at the time this circumstance was notified to **us** and **we** will regard this **claim** as having been notified under this Policy.

3. Additional insureds

We will indemnify any **third party** as an additional insured under this Policy, but only in respect of sums which they become legally obliged to pay (including liability for claimants' costs and expenses) as a result of a **claim** arising solely out of an act, error or omission committed by **you** or a **cyber event** discovered by **you**, provided that:

- a. **you** contracted in writing to indemnify the **third party** for the **claim** prior to it first being made against them; and
- b. had the **claim** been made against **you**, then **you** would be entitled to indemnity under this Policy

Before **we** indemnify any additional insured they must:

- a. prove to **us** that the **claim** arose solely out of an act, error or omission committed by **you** or a **cyber event** discovered by **you**; and
- b. fully comply with **CONDITION 1** as if they were **you**.

Where a **third party** is treated as an additional insured as a result of this Condition, any **claim** made by that **third party** against **you** will be treated by **us** as if they were a **third party** and not as an insured.

4. Cancellation

This Policy may be canceled with 30 days written notice by either **you** or **us**.

If **you** give **us** notice of cancellation, the return **premium** will be in proportion to the number of days that the Policy

is in effect, subject to a minimum retained amount of 30% of the **premium**. However, if **you** have made a claim under this Policy there will be no return **premium**.

If **we** give **you** notice of cancellation, the return **premium** will be in proportion to the number of days that the Policy is in effect.

We also reserve the right of cancellation in the event that any amount due to **us** by **you** remains unpaid more than 60 days beyond the **inception date**. If **we** exercise this right of cancellation it will take effect from 14 days after the date the written notice of cancellation is issued.

The Policy Administration Fee will be deemed fully earned upon inception of the Policy.

5. Continuous cover

If **you** have neglected, through error or oversight only, to report an incident discovered by **you** that might give rise to a **claim** under this Policy during the period of a previous renewal of this Policy issued to **you** by **us**, then provided that **you** have maintained uninterrupted insurance of the same type with **us** since the expiry of that earlier Policy, then, notwithstanding **EXCLUSION 9**, **we** will permit the matter to be reported under this Policy and **we** will indemnify **you**, provided that:

- a. the indemnity will be subject to the applicable limit of liability of the earlier Policy under which the matter should have been reported or the **policy limit** plus the **incident response limit**, whichever is the lower;
- b. **we** may reduce the indemnity entitlement by the monetary equivalent of any prejudice which has been suffered as a result of the delayed notification; and
- c. the indemnity will be subject to all of the terms, Conditions, Definitions and Exclusions of this Policy, other than a) above.

6. Extended reporting period

An extended reporting period of 60 days following the **expiry date** will be automatically granted at no additional premium. This extended reporting period will cover:

- a. **cyber events** first discovered by **you**;
- b. **claims** first made against **you**; and
- c. circumstances that a senior **executive officer** became aware of;

during the **period of the policy** and reported to **us** during this 60 day extended reporting period, subject to all other terms, conditions and exclusions of the policy. No **claim** will be accepted by **us** in this 60 day extended reporting period if **you** are entitled to indemnity under any other insurance, or would have been entitled to indemnity under such insurance but for its exhaustion.

7. Optional extended reporting period

If **we** or **you** decline to renew or cancel this Policy then **you** will have the right to have issued an endorsement providing an optional extended reporting period for the duration stated in the Declarations page which will be effective from the cancellation or non-renewal date. This optional extended reporting period will cover:

- a. **cyber events** first discovered by **you**;
- b. **claims** first made against **you**; and
- c. circumstances that a **senior executive officer** became aware of;

during the **period of the policy** and reported to **us** during this optional extended reporting period, subject to all other terms, conditions and exclusions of the Policy.

The right to the optional extended reporting period will not be available to **you** where cancellation or non-renewal by **us** is due to non-payment of the **premium** or **your** failure to pay any amounts in excess of the applicable **policy limit** plus the **incident response limit** or within the amount of the applicable **deductible** as is required by this Policy in the payment of claims.

At the renewal of this Policy, **our** quotation of different **premium, deductible**, limits of liability or changes in policy language will not constitute non-renewal by **us**.

8. Fraudulent claims

If **you** notify **us** of any claim knowing it to be false or fraudulent in any way, **we** will have no responsibility to pay that claim, **we** may recover from **you** any sums paid in respect of that claim and **we** reserve the right to terminate this Policy from the date of the fraudulent act. If **we** exercise this right **we** will not be liable to return any **premium** to **you**. However, this will not affect any claim under this Policy which has been previously notified to **us**.

9. Innocent non-disclosure

We will not seek to avoid the Policy or reject any claim on the grounds of non-disclosure or misrepresentation except where the non-disclosure or misrepresentation was reckless or deliberate.

10. Mergers and acquisitions

During the **period of the policy**, if **you** acquire another entity's assets or liabilities then **you** will have automatic coverage for any **claim** that falls under this Policy that arises directly or indirectly out of these assets or liabilities on the condition that:

- a. the value of the acquired entity's assets or liabilities are no more than 15% of **your** asset value; and
- b. the acquired entity's **business operations** are not materially different from **your business operations**;
- c. the acquired entity has not experienced a **cyber event** in the last three years;
- d. the acquired entity has not experienced a **claim** in the last three years; and
- e. **you** give **us** written notice within sixty days of completion of the acquisition.

Any coverage extended to the newly acquired entity will be effective from the date of acquisition. Under no circumstances will **we** make any payment under this policy for any **claim** arising from a **cyber event** experienced by the newly acquired entity which a **senior executive officer** was aware of, or ought reasonably to have been aware of, prior to the date of acquisition, including any **claim** or circumstance notified to any other insurer.

In the event that the above conditions are not met, **you** must provide **us** with all underwriting information requested,

obtain **our** express written agreement to extend coverage, and agree to any additional **premium** and terms of coverage required by **us** prior to the newly acquired entity being included under this Policy.

If during the **period of the policy** you consolidate, merge with or are acquired by another entity then all coverage under this Policy will terminate at the date of the consolidation, merger or acquisition unless **we** have issued an endorsement extending coverage under this Policy, and **you** have agreed to any additional **premium** and terms of coverage required by **us**.

11. Our duty to defend

We have the right and duty to take control of and conduct in **your** name the investigation, settlement or defense of any **claim**. **We** will not, however, have any duty to pay **costs and expenses** of any part of any **claim** that is not covered by this Policy.

We will always endeavor to settle any **claim** through negotiation, mediation or some other form of alternative dispute resolution and will pay on **your** behalf the amount **we** agree with the claimant. If **we** cannot settle using these means, **we** will pay the amount which **you** are found liable to pay either in court or through arbitration proceedings, subject always to the **policy limit** and **incident response limit**.

If **you** refuse to consent to a settlement **we** recommend and the claimant will accept, **you** may continue the defense and investigation of that **claim**. However, the further **costs and expenses** incurred will be paid by **you** and **us** on a proportional basis, with 80% payable by **us** and 20% payable by **you**. As a consequence of **your** refusal, **our** liability for any **claim**, excluding **costs and expenses**, will not be more than the amount that **we** could have settled the **claim** for had **you** consented.

12. Our rights of recovery

You must maintain all of **your** rights of recovery against any **third party** and make these available to **us** where possible.

We will not exercise any rights of recovery against any **employee** or **senior executive officer**, unless this is in respect of any fraudulent or dishonest acts or omissions as proven by final adjudication, arbitral tribunal or written admission by **you**.

Any recoveries will be applied in proportion to the amounts paid by **you** and **us**.

13. Prior subsidiaries

Should an entity cease to be a **subsidiary** after the **inception date**, cover in respect of the entity will continue as if it was still a **subsidiary** during the **period of the policy**, but only in respect of an act, error, omission or event occurring prior to the date that it ceased to be a **subsidiary**.

14. Process for adjustment of business interruption losses

In order to determine the amount of **loss** following an interruption to **your business operations** covered under **INSURING CLAUSE 3 (SECTION B)** only), the **cyber incident manager** will appoint an independent expert agreed between **you** and **us** which will be paid for by **us** in accordance with **INSURING CLAUSE 3 (SECTION D)** only).

If an independent expert cannot be agreed upon, one will be appointed by an arbitrator mutually agreed between **you** and **us** whose decision will be final and binding.

Once an independent expert has been appointed, their calculation of **loss** will be final and binding.

15. Process for paying privacy breach notification costs

Any **privacy breach** notification transmitted by **you** or on **your** behalf must be done with **our** prior written consent. **We** will ensure that notification is compliant with any legal or regulatory requirements and contractual obligations. No offer must be made for financial incentives, gifts, coupons, credits or services unless with **our** prior written consent which will only be provided if the offer is commensurate with the risk of harm.

We will not be liable for any portion of the costs **you** incur under **INSURING CLAUSE 1 (SECTION E)** only that exceed the costs that **you** would have incurred had **you** gained **our** prior written consent. In the absence of **our** prior written consent **we** will only be liable to pay **you** the equivalent cost of a notification made using the most cost effective means permissible under the governing law.

16. Choice of law and service of suit

In the event of a dispute between **you** and **us** regarding this Policy, the dispute will be governed by the laws of the State of the United States of America shown as the choice of law stated in the Declarations page. **We** agree, at **your** request, to submit to the jurisdiction of a court of competent jurisdiction within the United States of America.

Nothing in this Condition constitutes or should be understood to constitute a waiver of **our** rights to commence an action in any court of competent jurisdiction in the United States of America, to move an action to a United States District Court, or to seek a transfer of a case to another court as permitted by the laws of the United States of America or the laws of any State of the United States of America.

It is further agreed that service of process in such suit may be made upon the law firm stated in the Declarations page and that in any suit instituted against **us**, **we** will abide by the final decision of such court or of any appellate court in the event of an appeal. The law firm stated in the Declarations page is authorized and directed to accept service of process on **our** behalf in any such suit and, at **your** request, to give a written undertaking to **you** that they will enter a general appearance on **our** behalf in the event such suit is instituted.

Additionally, in accordance with the statute of any state, territory or district of the United States which makes such a provision, **we** hereby designate the Superintendent, Commissioner or Director of Insurance or other officer specified for that purpose in the statute, or his successor or successors in office, as **our** true and lawful attorney upon whom may be served any lawful process in any action, suit or proceeding instituted by **you** arising out of this Policy. The law firm stated in the Declarations page is hereby designated as the firm to whom the above mentioned officer is authorized to mail such process or a copy thereof.