

COALITION CYBER AND TECHNOLOGY POLICY 3.0

IMPORTANT NOTICES	
ABOUT COALITION	Coalition is the trading name of Coalition Insurance Solutions Pty Ltd ABN 33 657 140 791, Australian Financial Services Licence 539846, an insurance underwriting agency.
ABOUT THE INSURERS	This policy is co-underwritten by Allianz Australia Insurance Limited ABN 15 000 122 850 AFS Licence No. 234708 (Allianz), and HDI Global SE, Australia ABN 55 490 279 016 (HDI), the Australian branch of HDI Global SE, a company registered in German and Mitsui Sumitomo Insurance Company Limited (“MSI”), ABN 49 000 525 637, AFSL 240816 (together the Insurers). The Insurers are authorised general insurers in Australia, regulated by the Australian Prudential Regulation Authority, and are issuers of this Policy. Coalition Insurance Solutions Pty Ltd holds a binding authority from the Insurers to issue contracts of insurance, and to deal with or settle claims on behalf of the Insurers, as their agent.
SEVERAL LIABILITY	The liability of an insurer under this Policy is several and not joint with other insurers to this Policy or any other insurer that may underwrite this Policy. An insurer is liable only for the proportion of liability it has underwritten. The proportion of liability under this Policy underwritten by an insurer is shown next to its stamp.
CONTACT DETAILS	Coalition and the insurers can be contacted using the details below. Coalition Insurance Solutions Pty Ltd Phone: +(61) 261 898 062 Email: aus@coalitioninc.com Mail: Coalition, «pretty_address(coalition.address,» Allianz Australia Insurance Limited Mail: GPO Box 9870 Melbourne VIC 3000 Mitsui Sumitomo Insurance Company Limited Mail: Level 26, 135 King Street, Sydney, NSW 2000 Telephone: 02 9222 7600 Email: msiaus@ms-ins.com.au HDI Global SE, Australia Mail: Level 19, 20 Martin Place, Sydney, NSW 2000
YOUR DUTY OF DISCLOSURE	Before you enter into an insurance contract, you have a duty to tell us anything that you know, or could reasonably be expected to know, that may affect our decision to insure you and on what terms. You have this duty until the contract is entered into (or renewed, extended, varied or reinstated as applicable). You have the same duty before you renew, extend, vary or reinstate an insurance contract. You do not need to tell us anything that: • reduces the risk we insure you for; or • is common knowledge; or • we know in the ordinary course of our business or should know as an insurer; or • we waive your duty to tell us about
IF YOU DO NOT TELL US SOMETHING	If you do not tell us anything you are required to, we may cancel your contract or reduce the amount we will pay you if you make a claim, or both. If your

	failure to tell us is fraudulent, we may refuse to pay a claim and treat the contract as if it never existed.
GENERAL INSURANCE CODE OF PRACTICE	We are a signatory to the General Insurance Code of Practice (the Code) developed by the Insurance Council of Australia. The objectives of the Code are to further raise standards of service and promote customer confidence in the general insurance industry. Further information about the Code and your rights under it are available at www.codeofpractice.com.au and on request.
PRIVACY STATEMENT	Coalition, Allianz, HDI Global SE, Australia, and MSI are committed to protecting your privacy (jointly referred to as 'we' for the purposes of this section only). This statement provides you with an overview of how we collect your personal information and how we use it. You can obtain a copy of Coalition's Privacy Policy by visiting us at http://www.coalitioninc.com/. A copy of Allianz's full Privacy Policy is located at http://www.allianz.com.au/about-us/privacy. A copy of MSI's full Privacy Policy is located at http://www.msi-oceania.com/privacy/. A copy of HDI's full Privacy Policy is located at https://www.hdi.global/en-au/legal/privacy/ Collection, use and disclosure We usually collect your personal information when you interact with us (for example, when you apply for a policy or use our services). We may also collect your personal information from other sources, including when we scan the internet for cyber threats, through the use of cookies on our website and from third parties who may refer you to us. If you do not provide us with the personal information that we request, we may be unable to provide our products or services to you. We use the information we collect to • provide or fulfil services to you, • establish and verify your identity, handle and resolve transactions (including billing transactions), • provide insurance services (including activating, maintaining or servicing a policy), • maintain and improve our services and products (including to operate, develop and enhance them), • communicate with you about our products and services (including by sending announcements, updates, security alerts, and support and administrative messages), • tell you about products and services of our affiliates and business partners which we believe may be of interest to you, • respond to your queries, personalise your experience in using our products and services, • comply with legal and contractual requirements (including to facilitate audits, comply with our internal policies directed at compliance with such requirements, and comply with applicable law), • identify and manage unauthorised conduct or security threats (including to prevent, identify, investigate and deter fraudulent, unethical or illegal activity, including cyberattacks and identity theft), and • help you to respond to a cyber incident. We usually disclose your personal information to persons who help us to provide our products and services to you, and for the purposes described in the paragraph above. For example, we will disclose your information in connection with claims, for payment processing, third party service providers (who provide website development, hosting, maintenance, transcription etc), promotional partners and third party applications, our affiliates and related bodies corporate, to assist with a business transfer or to enforce our terms of use.

	We will sometimes disclose your personal information to recipients who are located overseas. For example, we use third party service providers in the U.S. and other jurisdictions. Where to find out more Our Privacy Policy www.coalitioninc.com/legal/privacy contains additional information about how we handle your personal information. The Privacy Policy also includes information about how you may access your personal information that we hold and seek correction of that information. Our Privacy Policy also includes information about how you may complain about a breach of the Australian Privacy Principles, or a registered code that binds us and how we will handle that complaint. If you have any questions, you can contact us at: privacy@coalitioninc.com
COMPLAINTS AND DISPUTE RESOLUTION	If you experience a problem or are not satisfied with our service or products, you can contact the Coalition Customer Success Phone: +(612) 6189 8062 Online: www.coalitioninc.com/en-au/contact Email: complaints@coalitioninc.com We will do our best to resolve the matter directly with you within 30 days of receiving it, in accordance with our dispute resolution procedures. We will keep you informed of the progress at least every 10 business days (unless we agree to an alternate timeframe). If you are unsatisfied with our response, you can refer the complaint to the Australian Financial Complaints Authority (AFCA) subject to its rules and time limits. AFCA is a free and independent external dispute resolution scheme approved by the Australian Securities and Investments Commission. We are a member of this scheme and we agree to be bound by its determinations about a dispute. If we do not respond to your complaint within 30 days, you can also refer your complaint to AFCA. We will tell you about this in writing and also the reasons for our delay. AFCA may be contacted at: Website: www.afca.org.au Telephone: 1800 931 687 (free call) Email: info@afca.org.au In writing to: Australian Financial Complaints Authority, GPO Box 3, Melbourne VIC 3001
FINANCIAL CLAIMS SCHEME	We and our agents are covered by the Financial Claims Scheme (FCS). This means that you may be entitled to compensation from the scheme in the unlikely event we cannot meet our obligations. The FCS is a government-backed safety net that covers most general insurance policies for claims up to \$5,000, with claims above \$5,000 eligible if they fulfil certain criteria. Once activated by the Australian government, FCS is administered by the Australian Prudential Regulation Authority. Further information about the scheme is available from the FCS: Website: apra.gov.au/financial-claims-scheme-0 Telephone: 1300 558 849 (in Australia, free call) or +61 2 8037 9015 (outside Australia) Email: info@apra.gov.au Post: Australian Prudential Regulation Authority GPO Box 9836

	Sydney NSW 2001 Australia
GST NOTICE	The Policy has a GST provision in relation to premium and our payment to you for claims. It may have an impact on how you determine the amount of insurance you need. Please read carefully. Seek professional advice if you have any queries about GST and your insurance. Sums Insured: All monetary limits in the Policy may be adjusted for GST in some circumstances (see below). Claim settlements – Where we agree to pay: When we calculate the amount we will pay you, we will have regard to the items below: Acquisition of goods, services or repairs Where you are liable to pay an amount for GST in respect of an acquisition relevant to your claim (such as services to repair a Damaged item insured under the Policy) we will pay for the GST amount. We will pay the GST amount in addition to the Sum Insured or Limit of Indemnity or other limits shown in the Policy or in the Schedule (unless we state GST is included in Sum Insured or Limit of Indemnity). If your Sum Insured or Limit of Indemnity is not sufficient to cover your loss, we will only pay the GST amount that relates to our settlement of your claim. We will reduce the GST amount we pay by the amount of any input tax credits to which you are or would be entitled. Payment as compensation Where we make a payment under the Policy as compensation instead of payment for a relevant acquisition, we will reduce the amount of the payment by the amount of any input tax credit that you would have been entitled to had the payment been applied to a relevant acquisition. Where the Policy insures business interruption, we will (where relevant) pay you on your claim by reference to the GST exclusive amount of any supply made by your business that is relevant to your claim. Disclosure – Input tax credit entitlement If you register, or are registered, for GST you are required to tell us your entitlement to an input tax credit on your premium. If you fail to disclose or you understate your entitlement, you may be liable for GST on a claim we may pay. The Policy does not cover you for this GST liability, or for any fine, penalty or charge for which you may be liable.
COOLING OFF	You can call us to cancel your Policy within 14 days from either: • the date we issued you a new Policy, or • or the start date of a Policy that you have renewed and in either of these situations, provided you have not made a claim or an event has not occurred that could give rise to a claim on your policy, we will refund your premium. We may deduct from your refund amount any government taxes or duties we cannot recover. In addition to your cooling off period, you can cancel the Policy at any time by calling us.

SECTION I	
INTRODUCTION	This Policy is a contract of insurance between the named insured and us. This Policy includes and must be read together with the Declarations page and any Endorsements. These set out your Limits of Liability and Retention and other matters that form part of this Policy. The insurance provided under this Policy for claims made against you, under Section II, THIRD PARTY LIABILITY COVERAGES, is on a claims made and reported basis, and applies to claims only if they are first made against you during the policy period (or any applicable Optional Extended Reporting Period) and reported to us in accordance with the terms of this Policy. In accordance with Section 40(3) of the Insurance Contracts Act 1984 (Cth), Section II, THIRD PARTY LIABILITY COVERAGES of this Policy may also respond to written notifications of facts that might give rise to a claim against you even if a claim has not yet been made against you. This notification must be given to us as soon as reasonably practicable after you become aware of the facts and prior to the expiry of the policy period. Claim expenses reduce the applicable Limits of Liability, are subject to retentions, and may exhaust the applicable Limits of Liability. Please note that the terms throughout this wording in bold lowercase print are defined terms and have special meaning as set forth in Section IX, DEFINITIONS.
SECTION II	
WHAT WE COVER – OUR INSURING AGREEMENTS	In consideration of the named insured's payment of the premium, in reliance upon the information provided to us, including in and with the submission, and subject to the Limits of Liability and applicable Retention(s), exclusions, conditions, and other terms of this Policy, we agree to provide the following insurance coverage provided that: 1. The event first took place after the retroactive date and before the end of the policy period; 2. For THIRD PARTY LIABILITY COVERAGES, the claim is made against you during the policy period (or any applicable Optional Extended Reporting Period), and is reported to us during the policy period or during any applicable extended reporting period; 3. For FIRST PARTY COVERAGES, the incident is first discovered by you during the policy period, and is reported to us during the policy period or any applicable extended reporting period; and 4. Notice is provided in accordance with Section IV, YOUR OBLIGATIONS AS AN INSURED.
THIRD PARTY LIABILITY COVERAGES	
THIRD PARTY SECURITY AND PRIVACY	
A. NETWORK AND INFORMATION SECURITY LIABILITY	We will pay on your behalf claim expenses and damages that you become legally obligated to pay resulting from a claim against you for a security failure, data breach, or privacy liability .
B. REGULATORY DEFENCE AND PENALTIES	We will pay on your behalf claim expenses and regulatory penalties that you become legally obligated to pay resulting from a claim against you in the form of a regulatory proceeding .
C. PCI FINES AND ASSESSMENTS	We will pay on your behalf claim expenses and PCI fines and assessments that you become legally obligated to pay resulting from a claim against you for a data breach compromising payment card data.
D. FUNDS TRANSFER LIABILITY	We will pay on your behalf claim expenses and funds transfer liability loss that you become legally obligated to pay resulting from a claim against you for a funds transfer liability .
TECHNOLOGY AND MEDIA PROFESSIONAL	

E. TECHNOLOGY ERRORS AND OMISSIONS	We will pay on your behalf claim expenses and damages that you become legally obligated to pay resulting from a claim against you for a technology and professional services wrongful act .
F. MULTIMEDIA CONTENT LIABILITY	We will pay on your behalf claim expenses and damages that you become legally obligated to pay resulting from a claim against you for a multimedia wrongful act .
FIRST PARTY COVERAGES	
EVENT RESPONSE	
G. BREACH RESPONSE SERVICES	We will pay on your behalf breach response services resulting from an actual or suspected security failure, data breach, cyber extortion, funds transfer fraud, or impersonation fraud , first discovered by you during the policy period .
H. BREACH RESPONSE COSTS	We will pay on your behalf breach response costs resulting from an actual or suspected security failure or data breach first discovered by you during the policy period .
I. CRISIS MANAGEMENT AND PUBLIC RELATIONS	We will pay on your behalf crisis management costs resulting from a public relations event first discovered by you during the policy period .
J. RANSOMWARE AND CYBER EXTORTION	We will pay on your behalf cyber extortion expenses resulting from cyber extortion first discovered by you during the policy period .
K. DIRECT AND CONTINGENT BUSINESS INTERRUPTION, AND EXTRA EXPENSES FROM SECURITY FAILURE AND SYSTEMS FAILURE	We will pay business interruption loss, contingent business interruption loss, and extra expenses that you incur during the indemnity period directly resulting from the partial or complete interruption of computer systems for a period longer than the waiting period caused by a security failure or systems failure first discovered by you during the policy period. The period of time set forth in Item 5.K. ii. Enhanced Waiting Period of the Declarations will be the waiting period for any interruption of computer systems caused by a denial of service attack where a Distributed Denial of Service mitigation vendor from our list of panel providers is utilised at the time of such denial of service attack.
L. PROOF OF LOSS PREPARATION EXPENSES	We will pay on your behalf proof of loss preparation expenses .
M. DIGITAL ASSET RESTORATION	We will pay on your behalf restoration costs that you incur because of the alteration, destruction, damage, theft, loss, or inability to access digital assets directly resulting from a security failure or systems failure first discovered by you during the policy period .
N. COMPUTER REPLACEMENT AND BRICKING	We will pay on your behalf computer replacement costs that you incur resulting from a security failure first discovered by you during the policy period .
O. REPUTATIONAL HARM LOSS	We will pay reputational harm loss that you incur during the reputation indemnity period solely and directly resulting from an adverse publication first published during the policy period specifically concerning a security failure, data breach, cyber extortion, or privacy liability first discovered by you and reported to us during the policy period. The reputation waiting period for any reputational harm loss will be the period of time set forth in Item 5.O. of the Declarations.
P. COURT ATTENDANCE	We will pay you court attendance costs set forth in Item 5.P.i. of the Declarations, subject to the maximum amount set forth in Item 5.P.ii. of the Declarations.
Q. CRIMINAL REWARD	We will pay on your behalf, in our reasonable discretion, criminal reward costs .

CYBER CRIME	
R. FUNDS TRANSFER FRAUD, PERSONAL FUNDS FRAUD, AND SOCIAL ENGINEERING	We will pay funds transfer loss that you incur resulting from a funds transfer fraud or personal funds fraud first discovered by you during the policy period .
S. SERVICE FRAUD INCLUDING CRYPTOJACKING	We will pay on your behalf service fraud loss that you incur resulting from a security failure first discovered by you during the policy period .
T. IMPERSONATION REPAIR COSTS	We will pay on your behalf impersonation repair costs that you incur resulting from an impersonation fraud first discovered by you during the policy period .
U. INVOICE MANIPULATION	We will pay you invoice manipulation loss that you incur resulting from any invoice manipulation first discovered by you during the policy period .
SECTION III	
EXCLUSIONS – WHAT IS NOT COVERED	This Policy does not apply to and we will not make any payment for any claim expenses, damages, funds transfer liability loss, loss, breach response costs, breach response services, regulatory penalties, PCI fines and assessments , or any other amounts directly or indirectly arising out of, resulting from, based upon, or attributable to:
A. BODILY INJURY	Any physical injury, sickness, disease, mental anguish, emotional distress, or death of any person, provided, however, that this exclusion will not apply to any claim for mental anguish or emotional distress under Sections II.A, NETWORK AND INFORMATION SECURITY LIABILITY and II.F, MULTIMEDIA CONTENT LIABILITY.
B. CONFISCATION	Confiscation, nationalisation, requisition, destruction of, or damage to any property, computer systems , software, or electronic data by order of governmental or public authority.
C. CONTRACTUAL LIABILITY	Any contractual liability or obligation or any breach of contract or agreement either oral or written, provided, however, that this exclusion will not apply: 1. with respect to the coverage provided by Section II.A, NETWORK AND INFORMATION SECURITY LIABILITY, and Section II.H, BREACH RESPONSE COSTS, to your obligations to maintain the confidentiality or security of personally identifiable information or third party corporate information; 2. with respect to the coverage provided by Section II.F., TECHNOLOGY ERRORS AND OMISSIONS, to any unintentional breach of a written contract to provide technology services or technology products; 3. With respect to the coverage provided by Section II.E, MULTIMEDIA CONTENT LIABILITY, to misappropriation of ideas under implied contract; 4. with respect to the coverage provided by Section II.C, PCI FINES AND ASSESSMENTS; or 5. to the extent you would have been liable in the absence of such contract or agreement.
D. DISCRIMINATION	Any discrimination of any kind in breach of any applicable laws.
E. EMPLOYMENT PRACTICES	Any employer-employee relations, policies, practices, acts, or omissions (including wrongful dismissal, discharge or termination, discrimination, harassment, retaliation or other employment-related claim). However, this exclusion will not apply to a claim by a current or former employee under Section II.A, NETWORK AND INFORMATION SECURITY LIABILITY or: 1. breach response services provided under Section II.G, BREACH RESPONSE SERVICES; or 2. breach response costs provided under Section II.H, BREACH RESPONSE COSTS;

	involving a security failure, data breach, cyber extortion, funds transfer fraud, or impersonation fraud , as applicable to coverage Sections II.G and H, that impacts current or former employees .
F. FRAUD BY A SENIOR EXECUTIVE	Any dishonest, fraudulent, criminal, or malicious act or omission of any senior executive or carried out with the knowledge of any senior executive. However, this exclusion does not apply to claim expenses incurred in defending any such claim until and unless a final, non-appealable adjudication (for example there are avenues for appeal of the relevant decision) establishes that a senior executive committed or had knowledge of such dishonest, fraudulent, criminal, or malicious act or omission, at which time the named insured will reimburse us for all claim expenses we have reasonably incurred or paid in defending such claim. This exclusion will not apply to any natural person insured who did not participate in or otherwise be involved in the dishonest, fraudulent, criminal, or malicious act or omission.
G. COURT ORDERS	Any court order or demand: 1. requiring you to provide personally identifiable information to any domestic or foreign law enforcement, administrative, regulatory, or judicial body or other governmental authority. However, this exclusion will not apply to any claim expenses, damages, and regulatory penalties that you become legally obligated to pay resulting from your response to a regulatory proceeding. 2. requiring the shutdown of systems or services.
H. ILLEGAL REMUNERATION	Any profit, remuneration, or advantage to which you are not legally entitled. However, this exclusion does not apply to claim expenses incurred in defending any such claim until and unless a final, non-appealable adjudication (for example there are avenues for appeal of the relevant decision) establishes the gaining of any profit, remuneration, or advantage to which you are not legally entitled, at which time the named insured will reimburse us for all claim expenses we incurred or paid in defending such claim.
I. INSURED VERSUS INSURED	Any claim made by or on behalf of: 1. an insured under this Policy or by a stockholder or member in their capacity as such against an insured; however, this exclusion will not apply to an otherwise covered claim made by: a. an employee arising from a security failure or data breach; or b. an additional insured; 2. any business enterprise in which you have greater than a twenty percent (20%) ownership interest; or 3. any parent company or other entity that owns more than twenty percent (20%) of an insured.
J. INTELLECTUAL PROPERTY	Violation or infringement of any intellectual property right or obligation, including: 1. infringement of copyright of software, firmware, or hardware; 2. distribution or sale of, or offer to distribute to sell, any goods, products, or services; 3. other use of any goods, products, or services that infringes or violates any intellectual property law or right relating to the appearance, design, or function of any goods, products, or services; or 4. misappropriation, misuse, infringement, or violation of any patent, patent right, or trade secret; however, this exclusion will not apply to: 1. Section II.E, TECHNOLOGY ERRORS & OMISSIONS for any claim alleging that any software code or software products provided as part

	of your technology services or technology products violate another party's copyright described in items 1, 2, or 3 above; or 2. Section II.F, MULTIMEDIA CONTENT LIABILITY, for an otherwise covered claim for a multimedia wrongful act, provided that, this exception to exclusion K. INTELLECTUAL PROPERTY will not apply to any violation or infringement of any intellectual property right or obligation described in items 1 and 4 above.
K. MERCHANT LIABILITY	Any charge back, interchange fee, discount fee, service related fee, rate, or charge; or liability or fee incurred by you due to a merchant service provider, payment processor, payment card company, or bank reversing or freezing payment transactions, except that this exclusion will not apply to coverage afforded under Section II.C, PCI FINES AND ASSESSMENTS.
L. NATURAL DISASTER	Any physical event or natural disaster, including but not limited to fire, flood, earthquake, volcanic eruption, explosion, lightning, wind, hail, tidal wave, and landslide.
M. NUCLEAR	Any exposure or threatened exposure to any radioactive matter or any form of radiation or contamination by radioactivity of any kind or from any source, including any nuclear reaction, nuclear radiation, or radioactive contamination from any kind of nuclear fuels, waste or the combustion or ignition of nuclear fuel. This exclusion applies regardless of whether any other causes, events, materials, or products contributed concurrently or in any sequence to the claim or event , or the liability or legal obligation alleged or existing.
N. POLLUTANTS	Any: 1. discharge, dispersal, seepage, migration, release, or escape of pollutants, or any threatened discharge, seepage, migration, release, or escape of pollutants; or 2. request, demand, order, or statutory or regulatory requirement that you or others detect, report, test for, monitor, clean up, remove, remediate, contain, treat, detoxify, or neutralise, or in any way respond to, or assess the effects of pollutants; including any claim, suit, notice, or proceeding by or on behalf of any governmental authority or quasi-governmental authority, a potentially responsible party or any other person or entity for any amounts whatsoever because of detecting, reporting, testing for, monitoring, cleaning up, removing, remediating, containing, treating, detoxifying, or neutralising, or in any way responding to, or assessing the effects of pollutants. This exclusion applies regardless of whether any other causes, events, materials, or products contributed concurrently or in any sequence to the claim or event, or the liability or legal obligation alleged or existing.
O. PRIOR KNOWLEDGE	1. any event, act, error, or omission that any senior executive on or before the continuity date knew or could have reasonably foreseen might be the basis of a claim, loss, breach response costs, or breach response services under this Policy; or 2. any claim, event, or circumstance which has been the subject of any notice given to the insurer of any other policy in force prior to the inception date of this policy period.
P. RETROACTIVE DATE	Any event , act, error, or omission that took place prior to the retroactive date , or any related or continuing acts, errors, omissions, or events where the first such act, error, omission, or event first took place prior to the retroactive date .
Q. SECURITIES	The ownership, sale or purchase of, or the offer to sell or purchase stock or other securities (such as bonds or promissory notes).
R. TANGIBLE PROPERTY	Any injury or damage to, destruction, impairment, or loss of use of any tangible property , including any computer hardware rendered unusable by a security failure or systems failure , except this exclusion will not apply to coverage afforded under Section II.N, COMPUTER REPLACEMENT AND BRICKING.

S. TECHNOLOGY ERRORS AND OMISSIONS EXCLUSIONS	With respect to the coverage provided by Section II.E., TECHNOLOGY ERRORS AND OMISSIONS, any: 1. breach of: a. express warranty or representation, except for an agreement to act or perform with a degree of skill and care as is consistent with applicable industry standards; b. other contractual obligation which goes beyond an express or implied duty to exercise a degree of skill and care as is consistent with applicable industry standards; or c. guarantee or any promises of cost savings, profits, or return on investment; 2. delay in delivery or performance, or failure to deliver or perform at or within an agreed upon period of time, however this exclusion will not apply if such delay or failure to deliver or perform is the result of a technology and professional services wrongful act, provided that you have made diligent efforts to deliver the applicable technology products or perform the applicable technology services; 3. inaccurate, inadequate, or incomplete description of the price of goods, products, or services; 4. cost guarantee, cost representation, or contract price estimate of probable costs or cost estimate actually or allegedly being exceeded; 5. commercial decision by you to stop providing any product or services; 6. provision of any sweepstakes, gambling activities, or lotteries, or price discounts, prizes, awards, money, or valuable consideration given in excess of a total contract or expected amount; 7. idea, trade secret, or confidential information that came into possession of any person or entity before such person or entity became an employee, board member, trustee, director, or officer of the named insured or any subsidiary; 8. unauthorised or surreptitious collection of any information by you, or failure to provide adequate notice that such information is being collected, or failure to comply with any legal requirement to provide individuals with the ability to consent or withhold consent for such collection; 9. loss, theft, or transfer of funds, monies, or securities in your care, custody, or control, or in the care, custody, or control of any third party for whom you are legally liable; 10. unfair competition, false or misleading advertising, or violation of consumer protection laws; or 11. costs or expenses incurred by you or others to withdraw, recall, repair, replace, upgrade, supplement, or remove any technology products or any products that contain or incorporate technology products or technology services. 12. Any withdrawal, recall, inspection, adjustment, removal, or disposal of any property, tangible or intangible, including computer systems and their component parts, mobile devices, and mechanical equipment.
T. THIRD PARTY MECHANICAL FAILURE	Electrical, mechanical failure, or interruption (including blackouts, brownouts, power surge, or outage) of a third party who owns or controls the supply of services, including telecommunications and other communications, GPS infrastructure, any core element of the internet or internet service, website hosts, server services, satellite, cable, electricity, gas, water, or other utility or power service providers. However, this exclusion will not apply to coverage under Section II.K, DIRECT AND CONTINGENT BUSINESS INTERRUPTION, AND EXTRA EXPENSES FROM SECURITY FAILURE AND SYSTEMS FAILURE, where such loss arises directly from a service provider directly experiencing their own security failure.

U. UNFAIR TRADE PRACTICE	Any false, unlawful, deceptive, anti-competitive or unfair trade practices; however, this exclusion does not apply to a claim under Section II.B, REGULATORY DEFENCE AND PENALTIES arising from a security failure or data breach .
V. VIOLATION OF ACTS/LAWS	Any violation of: 1. Corporations Act 2001 (Cth); 2. Superannuation Industry (Supervision) Act 1993(Cth); 3. Competition and Consumer Act 2010 (Cth); 4. Spam Act 2003 (Cth); 5. Criminal Code Act 1995 (Cth); 6. the Employee Retirement Income Security Act of 1974 (ERISA); 7. the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Act of 1940, or any other federal, provincial, territorial, or state securities laws; 8. the Organised Crime Control Act of 1970 (RICO); 9. the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM); 10. Telephone Consumer Protection Act (TCPA); 11. the Sherman Anti-Trust Act, the Clayton Act, or any price fixing, restraint of trade, or monopolisation statutes; 12. any similar local, state, federal, common, or foreign laws or legislation to the laws described in 6. through 11. however, this exclusion will not apply to a claim against you: 1. for any violation of the Corporations Act 2001 (Cth), Superannuation Industry (Supervision) Act 1993 (Cth), or Competition and Consumer Act 2010 (Cth), arising out of an alleged security failure, data breach, or privacy liability; 2. alleging a data breach or privacy liability in violation of U.S Securities and Exchange Commission (SEC) regulation S-P (17 C.F.R. § 248); or 3. for any violation of Australian federal, state or territory legislation regulating privacy or the disclosure of personal information including but not limited to the Privacy Act 1988 (Cth).
W. WAR	1. war 2. A cyber operation that is carried out as a part of a war; or 3. A cyber operation that causes a sovereign state to become an impacted state. Provided, however, item three (3) above shall not apply to the direct or indirect effect of a cyber operation on a computer system used by the insured or its third party service providers that is not physically located in an impacted state but is affected by a cyber operation. For the purpose of exclusion W. War, computer system means any computers and related peripheral components (including Internet of Things (IoT) devices), systems and applications software, terminal devices, related communications networks, mobile devices (handheld and other wireless computing devices), and storage and back-up devices.
X. WRONGFUL COLLECTION	1. Any actual or alleged violation of the Illinois Biometric Information Privacy Act or any similar federal, state, common, or foreign law; or 2. Any actual or alleged: (a) wiretapping or eavesdropping; (b) use of web beacons, tracking pixels or other software tools by you or on your behalf that wrongfully acquires, collects, tracks or shares an individual's activity, information or data; or (c) wrongful collection or use of personally identifiable information by you or on your behalf, except this subpart (2)(c) shall not apply to SECTION II.A NETWORK AND INFORMATION SECURITY for an otherwise covered claim under item 2 in the definition of privacy liability
SECTION IV	

YOUR OBLIGATIONS AS AN INSURED	
WHEN THERE IS A CLAIM OR EVENT	It is a condition of this Policy that you must provide us written notice of: 1. any claim; or 2. any incident that may result in a loss under Section II FIRST PARTY COVERAGES through the persons named in Item 9. of the Declarations as soon as reasonably practicable once such claim or incident is known to a senior executive. In no event will such notice to us be later than (i) the end of the policy period; or (ii) 90 days after the end of the policy period for claims made against you or incidents first discovered by you, in the last 60 days of the policy period. In the event of an adverse publication, such notice will include complete details of the adverse publication and date you first became aware of such adverse publication.
DUTY TO COOPERATE	When we assess your claim, we may undertake an investigation that we deem to be reasonably necessary, and you will cooperate with us in all reasonable investigations, respond to reasonable requests for information, and execute all papers and render assistance as reasonably requested by us. You will not knowingly or recklessly do anything that increases our exposure under this Policy. You will also cooperate with us and counsel in the defence of all claims and response to all events, and provide all information reasonably required for appropriate and effective representation. With respect to Section II.J, RANSOMWARE AND CYBER EXTORTION, you must make every reasonable effort not to divulge the existence of this coverage, without first seeking our prior consent (which we will not unreasonably withhold) except to the extent you are required by law to disclose the existence of this coverage in which case you will notify us of such disclosure as soon as reasonably practicable.
OBLIGATION TO NOT INCUR ANY EXPENSE OR ADMIT LIABILITY	You will not, except at your own cost, admit liability, make any payment, assume any obligation, incur any expense, enter into any settlement, stipulate to any judgement or award, or dispose of any claim without our prior written consent, such consent not to be unreasonably withheld, delayed or conditioned except as specifically provided in Section V, CLAIMS PROCESS. Compliance with a breach notice law will not be considered as an admission of liability for purposes of this paragraph. Expenses incurred by you in assisting and cooperating with us do not constitute claim expenses, loss, breach response costs, or breach response services under this Policy.
CONFIDENTIALITY	You will not publish or disclose the existence of this Policy or any Limits of Liability or Retentions, to any third party, including disclosure on your website or in your annual report, unless: 1. we provide our consent in writing, such consent not to be unreasonably withheld, delayed or conditioned; 2. you are reasonably required to provide a certificate of insurance; or 3. you are required to by court order
OBLIGATION TO PRESERVE OUR RIGHT OF SUBROGATION	In the event of any payment by us under this Policy, to the extent permitted by law we will be subrogated to all of your rights of recovery. You will provide us with reasonable assistance and cooperation to secure and preserve such subrogation rights, including the execution of any documents necessary to enable us to bring suit in your name. You will not knowingly or recklessly do anything after an event or other circumstance giving rise to a claim, loss, breach response costs, breach response services, regulatory penalties, or PCI fines and assessments to prejudice such subrogation rights without first obtaining our consent, such consent not to be unreasonably withheld, delayed or conditioned.

	This obligation does not apply to the extent that the right to subrogate is waived by you under a written contract with that person or organisation, prior to the event or other circumstance giving rise to the claim or loss.
AUTHORISATION OF NAMED INSURED TO ACT ON BEHALF OF ALL INSURED S	It is agreed that the named insured will act on behalf of all insureds with respect to the giving of notice of a claim, giving and receiving of notice of cancellation and non-renewal, payment of premiums and receipt of any return premiums that may become due under this Policy, receipt and acceptance of any endorsements issued to form a part of this Policy, exercising or declining of the right to tender the defence of a claim to us, and exercising or declining to exercise of any right to an Optional Extended Reporting Period. Where there is more than one named insured listed in Item 1 of the Policy Declarations or by endorsement to this Policy, then for the purpose of this clause only, the named insured is deemed to be the first entity listed under Item 1 of the Policy Declarations.
SECTION V	
CLAIMS PROCESS	
DEFENCE	We will have the right and duty to defend, subject to the Limits of Liability and applicable Retention(s), exclusions, conditions, and other terms of this Policy: 1. any claim against you seeking damages that are payable under the terms of this Policy; or 2. under Section II.B, REGULATORY DEFENCE AND PENALTIES, any claim in the form of a regulatory proceeding. You have the right to select defence counsel from our panel providers. If you would like to retain defence counsel not on our list of panel providers, such counsel must be mutually agreed upon between you and us, which agreement will not be unreasonably withheld or conditioned, and subject to you ensuring that the provider fee rate structure you've received is reasonable or not substantially different to our panel providers. We will pay claim expenses incurred with our prior written consent with respect to any claim seeking damages, funds transfer liability loss, or regulatory penalties payable under this Policy. We will have no obligation to pay claim expenses until you have satisfied the applicable Retention. The Limits of Liability of this Policy will be reduced and may be completely exhausted by payment of claim expenses. Our duty to defend ends once the applicable Limit of Liability is exhausted, or after deposit of the amount remaining on the applicable Limit of Liability in a court of competent jurisdiction. Upon such payment, we will have the right to withdraw from the defence of the claim.
RIGHT TO ASSOCIATE	We have the right, but not the duty, to request that we are involved in the investigation and response to any event or claim, including participation in the formation of strategy and review of forensic investigations and reports.
PRE-CLAIM ASSISTANCE	If in accordance with the Insurance Contracts Act 1984 (Cth) we are provided with notice of an act or other circumstance that is not yet a claim under Section IV, YOUR OBLIGATIONS AS AN INSURED, and you request assistance to mitigate against any potential future claim or incident covered under Section II WHAT WE WILL COVER - OUR INSURING AGREEMENTS, we may, in our discretion, agree to pay for up to the amount shown in Item 6. of the Declarations for legal, forensic, and IT services provided by a third party. Any such fees must be incurred with our prior consent by legal counsel or a consultant we have mutually agreed upon, our agreement will not be unreasonably withheld. If there is a subsequent covered claim made, or covered incident, then such legal counsel's and consultant's fees will be considered claim expenses, loss, breach response costs, or breach response services and will be subject to the applicable Limits of Liability and the Aggregate Policy Limit of Liability.

SETTLEMENT	If you refuse to consent to any settlement or compromise of a claim recommended by us and acceptable to the claimant and that does not unreasonably impose a burden on you, our liability for such claim will not exceed: 1. the amount for which such claim could have been settled, less the retention, plus claim expenses incurred up to the time of such refusal; and 2. seventy percent (70%) of claim expenses incurred after such settlement was refused by you, plus seventy percent (70%) of damages and regulatory penalties in excess of the amount such claim could have been settled under such settlement. In this event, we will have the right to withdraw from the further defence of such claim by tendering control of the defence thereof to you. The operation of this paragraph will be subject to the Limits of Liability and Retention provisions of this Policy.
SETTLEMENT WITHIN RETENTION	We agree that you may settle any claim where the total claim expenses, loss, damages, breach response costs, breach response services, regulatory penalties, and PCI fines and assessments do not exceed the applicable Retention, provided the entire claim is resolved and you obtain a full release from all claimants for any future liability arising out of, or in connection with, the same circumstances as that claim.
PROOF OF LOSS	With respect to business interruption loss, contingent business interruption loss, extra expenses, and reputational harm loss, you must complete and sign a written, detailed, and affirmed proof of loss within 90 days after your discovery of the security failure, systems failure, or adverse publication (unless such period has been extended by the underwriters in writing) which will include, at a minimum, the following information to the extent known or reasonably ascertainable by you: 1. full description of the circumstances, including the time, place, and cause of the loss; and 2. a detailed calculation of any business interruption loss, contingent business interruption loss, extra expenses, and reputational harm loss; and all underlying documents and materials that reasonably relate to or form part of the basis of the proof of such business interruption loss, contingent business interruption loss, extra expenses, and reputational harm loss. Any costs you incur in connection with establishing or proving business interruption loss, contingent business interruption loss, extra expenses, or reputational harm loss, including preparing a proof of loss, in excess of the Limits of Liability under Section II.L, Proof Of Loss Preparation Expenses, if purchased, will be your obligation and are not covered under this Policy. Solely with respect to verification of business interruption loss, contingent business interruption loss, and reputational harm loss, you agree to allow us to examine and audit your books and records that relate to this Policy during business hours at any time during the policy period and up to 12 months following our receipt of any proof of loss in accordance with this section.
SECTION VI	
LIMITS OF LIABILITY AND RETENTION	
LIMITS OF LIABILITY	<u>Aggregate Policy Limit of Liability and Limits of Liability for All Insuring Agreements Other Than Breach Response Services</u> The Aggregate Policy Limit of Liability set forth in Item 4. of the Declarations is the maximum amount we will be liable to pay for all claim expenses, damages, funds transfer liability loss, loss, breach response costs, PCI fines and assessments, regulatory penalties, and other amounts under this Policy, regardless of the number of claims, events, or insureds. The reference to

	Aggregate Policy Limit of Liability herein also refers to each participating Insurer's individual Quota Share Limit of Liability as stated in Item 8. of the Declarations. The Per Event Limit of Liability set forth in Item 4. of the Declarations is the maximum amount we will be liable to pay for all claim expenses, damages, funds transfer liability loss, loss, breach response costs, PCI fines and assessments, regulatory penalties, and other amounts arising from a single event under all Insuring Agreements, regardless of the number of Insuring Agreements triggered, claims, or insureds. Such Limits of Liability are part of, and not in addition to, the Aggregate Policy Limit of Liability. The Limit stated in Item 5. of the Declarations with respect to an Insuring Agreement is the maximum amount we will be liable to pay for all claim expenses, damages, funds transfer liability loss, loss, breach response costs, PCI fines and assessments, regulatory penalties, and other amounts arising from a single event and in aggregate for all events under that Insuring Agreement. Such Limits of Liability are part of, and not in addition to, the Aggregate Policy Limit of Liability. Our Limits of Liability for an Optional Extended Reporting Period, if applicable, will be part of, and not in addition to the Aggregate Policy Limit of Liability set forth in Item 4. of the Declarations. <u>Limit of Liability for Breach Response Services</u> Breach response services will be provided for a maximum of 72 hours following your notification to the breach response services advisor. Breach response services will be provided in addition to and will not erode the Aggregate Policy Limit of Liability.
RETENTION	We will only be liable for those amounts payable under this Policy which are in excess of the applicable Retention(s). Such Retention(s) cannot be insured. In the event that damages, funds transfer liability loss, PCI fines and assessments, regulatory penalties, claim expenses, breach response costs, breach response services, loss, or other amounts arising out of a claim or event are subject to more than one Retention, the Retention for each applicable insuring agreement will apply separately, provided that the sum of such Retention amounts will not exceed the largest applicable Retention amount. In the event that you elect to use Coalition Incident Response to provide computer forensic professional services, and Coalition Incident Response is available to provide such services, then any fees, costs and expenses of Coalition Incident Response for computer forensic professional services that result in covered breach response costs, claim expenses, cyber extortion expenses, or restoration costs, under the terms and conditions of this Policy will not be subject to any Retention. The Aggregate Retention set forth in Item 4. of the Declarations is the maximum amount you will be liable to pay towards satisfying Retentions for covered claims or events. Once the Aggregate Retention is paid, we will be liable for amounts payable under this Policy. Such amounts are part of and not in addition to the Limits of Liability of this Policy.
SECTION VII	
CANCELLATION AND OPTIONAL EXTENDED REPORTING PERIOD	
CANCELLATION	We may cancel this Policy at any time for non-payment of premium, or if you have made a fraudulent claim, by giving written notice to the named insured or your insurance broker at the address shown in Item 1. of the Declarations or by emailing written notice to an email address provided by you.

	The written notice shall state when the cancellation will be effective. Such cancellation will not be effective less than ten (10) days after such notice is mailed and will be made in accordance with the Insurance Contracts Act 1984 (Cth). Right to refund of premium: 1. For non-payment of premium the earned premium will be computed pro rata but the premium will be deemed fully earned if any claim, event, or any circumstance that could reasonably be expected to give rise to a claim or event, is reported to us on or before the date of cancellation. 2. For fraudulent claims, we need not return any of the premiums paid under this Policy and the further consequences set out in Section VII FRAUDULENT CLAIMS shall apply. Cancellation by the named insured: The named insured may cancel this Policy by surrender of this Policy to us or written notice to us stating when thereafter such cancellation will be effective. Furthermore: 1. Where permitted by applicable law, the named insured may provide such written notice of cancellation by electronic transmission. 2. The earned premium will be computed pro rata but the premium will be deemed fully earned if any claim, event, or any circumstance that could reasonably be expected to give rise to a claim or event, is reported to us on or before the date of cancellation. 3. Unless cancelled during the cooling off period, the policy fee shall be deemed to be fully earned and no refund will be provided.
FRAUDULENT CLAIMS	If you make a fraudulent claim under this Policy then we may be entitled to: 1. refuse the claim in whole or in part; 2. recover from you any sums paid to you in respect of the claim; and 3. cancel this Policy in accordance with Section VII CANCELLATION AND NON-RENEWAL.
OPTIONAL EXTENDED REPORTING PERIOD	In the event of cancellation or non-renewal of this Policy, by either the named insured or us, for reasons other than fraud or breach of the duty of disclosure or non-payment of premium or amounts within the applicable Retention, the named insured will have the right, upon payment in full of additional premium, to purchase an Optional Extended Reporting Period under this Policy, subject to all terms, conditions, limitations of, and any endorsements to this Policy, for a period of either: a. one year for an additional premium of 100% of the total annual premium; b. two years for an additional premium of 150% of the total annual premium; c. three years for an additional premium of 200% of the total annual premium; d. four years for an additional premium of 225% of the total annual premium; or e. five years for an additional premium of 250% of the total annual premium following the effective date of such cancellation or non-renewal. Such Optional Extended Reporting Period applies only to a claim first made against you during the Optional Extended Reporting Period and reported to us during the Optional Extended Reporting Period, and arising out of any actual or alleged act, error, or omission committed on or after the retroactive date and before the end of the policy period (or, if applicable, before the effective date

	of the Change in Control in Section VIII), subject to the Retention, Limits of Liability, exclusions, conditions, and other terms of this Policy. The Optional Extended Reporting Period will terminate on the effective date and hour of any other insurance issued to the named insured or the named insured's successor that replaces in whole or in part the coverage afforded by the Optional Extended Reporting Period. The named insured's right to purchase the Optional Extended Reporting Period must be exercised in writing no later than ninety (90) days following the cancellation or non-renewal date of this Policy, and must include payment of premium for the applicable Optional Extended Reporting Period as well as payment of all premiums due to us. If such written notice is not given to us, the named insured will not, at a later date, be able to exercise such right. At the commencement of any Optional Extended Reporting Period, the entire premium thereafter will be deemed earned and in the event the named insured terminates the Optional Extended Reporting Period before its expiring date, we will not be liable to return any portion of the premium for the Optional Extended Reporting Period. The fact that the time to report claims under this Policy may be extended by virtue of an Optional Extended Reporting Period will not in any way increase the Limits of Liability, and any amounts incurred during the Optional Extended Reporting Period will be part of, and not in addition to the Limits of Liability as stated in the Declarations. The Optional Extended Reporting Period will be renewable at our sole option.
SECTION VIII	
OTHER PROVISIONS	
CHANGE IN CONTROL	If during the policy period: - the named insured: (i) merges or consolidates with or into another entity, such that the named insured is not the surviving entity; or (ii) is acquired by another entity; or (iii) sells more than 50% of its assets to another entity, such that named insured is not the surviving entity; or - another entity or person, or group of affiliated entities or persons acting in concert, acquires securities or voting rights which result in ownership or voting control by the other organisation(s) or person(s) of more than 50% of the outstanding voting stock or voting rights representing the present right to vote for the election of directors, trustees, managers (if a limited liability company), or the equivalent executive management functions of the named insured; (items 1 and 2 above both referred to as a “Change in Control”), then this Policy will continue to remain in effect until the end of the policy period, but only with respect to any event, act, error, or omission that first occurred prior to the Change in Control. There will be no coverage provided by this Policy for any event, act, error, or omission occurring after the Change in Control. The named insured must give written notice of a Change in Control to us as soon as practicable, but no later than thirty (30) days after the Change in Control. The full premium for this Policy will be deemed to be fully earned immediately upon the date of the Change in Control. The above provision may be waived in writing by us.
CHOICE OF LAW AND JURISDICTION	This Policy shall be governed by and construed in accordance with the laws of New South Wales, Australia. Each party irrevocably agrees that the courts of New South Wales, Australia shall have exclusive jurisdiction over any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this agreement or its subject matter or formation.

NO ASSIGNMENT	No change in, modification of, or assignment of interest under this Policy will be effective except when made by written endorsement signed by us .
NON-PERMISSIBLE INSURANCE	Where we may not permissibly insure, either on an admitted or non-admitted basis, any entity that falls within the definition of an insured under this Policy, by virtue of the entity's domicile (or deemed location of risk for regulatory purposes), we will indemnify the named insured in respect of any loss to its insurable financial interest in such uninsured entity by way of agreed valuation calculated as the amount that we would have been liable to pay such uninsured entity for the applicable loss under the terms and conditions of this Policy had it been permissible to insure such uninsured entity.
OTHER INSURANCE	Subject to the Insurance Contracts Act 1984 (Cth), this Policy will apply excess of any other valid and collectible insurance available to you, (including the self-insured retention or deductible portion of that insurance), including an insurance specified as an underlying policy in any endorsement attached to this policy. This clause does not apply to Section II, G. BREACH RESPONSE SERVICES and H. BREACH RESPONSE COSTS.
REFERENCES TO LEGISLATION	Legislation referenced in this Policy includes subsequent Legislation . Any term used in this Policy and defined by reference to legislation will have the meaning given in any replacement definition or definition with materially the same object or purpose in subsequent Legislation .
SANCTIONS	Irrespective of any other provision of the Policy, we shall not be deemed to provide cover and we shall not be liable to pay any claim, claim expenses, damages, funds transfer liability loss, loss, breach response costs, breach response services, regulatory penalties, PCI fines and assessments or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim, claim expenses, damages, funds transfer liability loss, loss, breach response costs, breach response services, regulatory penalties, PCI fines and assessments or provision of such benefit would contravene or otherwise expose us to any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of Australia, the European Union, United Kingdom, Japan or United States of America.
TERRITORY – THE UNIVERSE	This Policy will apply to events occurring, claims made, and damages, losses, breach response costs, breach response services, regulatory penalties, and PCI fines and assessments incurred, anywhere in the universe.
TITLES	The titles and headings to the various sections, subsections, and endorsements of this Policy are included solely for ease of reference and do not limit coverage, expand coverage, or otherwise affect the provisions of such sections, subsections or endorsements.
SECTION IX	
DEFINITIONS	Words and phrases that appear in lowercase bold in this Policy have the meanings set forth below:
Adverse publication	means any report or communication to the public through any media channel including television, print media, radio, the internet, or electronic mail, of information that was previously unavailable to the public, specifically concerning a security failure, data breach, cyber extortion, or privacy liability that affects your customers or clients. All adverse publications relating to the same security failure, data breach, cyber extortion, or privacy liability will be deemed to have occurred on the date of the first adverse publication for the purposes of determining the applicable reputation waiting period and reputation indemnity period , and will be deemed to constitute a single reputational harm loss .
Breach notice law	means any statute or regulation, including from Australia, the UK, Canada, the United States, the European Union, or other country that requires: (i) notice to persons whose personally identifiable information was, or reasonably

	considered likely to have been accessed or acquired by an unauthorised person; or (ii) notice to regulatory agencies of such incident.
Breach response costs	means the following reasonable costs you incur with our prior written consent (which we will not unreasonably withhold) in response to an actual or suspected security failure or data breach: 1. computer forensic professional fees and expenses to determine the cause and extent of a security failure or data breach; 2. computer forensic professional fees for reasonable efforts to close off the point(s) of unauthorised entry and to terminate a security failure event. 3. costs to notify individuals affected or reasonably believed to be affected by such data breach, including printing costs, publishing costs, postage expenses, call centre costs, and costs of notification via phone or e-mail; 4. costs to provide government mandated public notices related to such security failure or data breach; 5. legal fees and expenses to advise you in connection with your investigation of a security failure or data breach and to determine whether you are legally obligated under a breach notice law to notify applicable regulatory agencies or individuals affected or reasonably believed to be affected by such security failure or data breach; 6. legal fees and expenses to advise you in complying with Payment Card Industry ("PCI") operating regulation requirements for responding to a data breach compromising payment card data, and the related requirements under a merchant service agreement, including a PCI forensic investigator when required under such merchant service agreement (this clause does not include any fees or expenses incurred in any legal proceeding, arbitration, or mediation, for any advice in complying with any PCI rules or regulations other than for assessment of PCI fines and assessments for a covered data breach, or to remediate the breached computer systems); 7. costs to provide up to two years (or longer if required by law) of a credit or identity monitoring program, including credit freezing and thawing, to individuals affected by such data breach; and 8. identity theft restoration services to those natural persons identified by a licensed identity theft investigator as victims of identity theft affected by such data breach. Breach response costs must be incurred within one year of your discovery of an actual or suspected security failure or data breach. You have our prior consent to incur breach response costs in the form of computer forensic fees under paragraph 1. and legal fees under paragraphs 5. and 6. with any vendor on our list of panel providers.
Breach response services	means the following services to assist with your initial response to an actual or suspected security failure, data breach, cyber extortion, funds transfer fraud, or impersonation fraud: 1. access to the 24/7 breach response hotline detailed in Item 9. of the Declarations; 2. two hour consultation and advice by legal counsel from our panel providers; 3. consultation and advice by the breach response services advisor; 4. preliminary forensics and threat intelligence gathered by and known to the breach response services advisor; and 5. Initial remote support and assistance provided by the breach response services advisor. Breach response services apply only to the initial assistance provided by the breach response services advisor and the two-hour consultation with legal counsel from our panel providers, and solely with respect to your initial response to an actual or suspected security failure, data breach, cyber extortion, funds transfer fraud, or impersonation fraud based upon the

	information provided by you to us and/or the breach response services advisor at the time you first notify us of the applicable security failure, data breach, cyber extortion, funds transfer fraud, or impersonation fraud. Breach response services are available only during the 72 hour time period following notification of the actual or suspected security failure, data breach, cyber extortion, funds transfer fraud, or impersonation fraud to the breach services advisor, and do not include the costs and expenses of any services which are covered under any other First Party Coverage of this Policy.
Breach response services advisor	means the entity(ies) or person(s) named in Item 14. of the Declarations.
Business interruption loss	means: 1. the net profit that would have been earned before taxes on income, or net loss that would not have been incurred, directly due to the partial or complete interruption of computer systems; and 2. continuing normal operating expenses (including payroll), but only to the extent that such operating expenses must necessarily continue during the indemnity period. Provided, however, that business interruption loss will not include net profit that would likely have been earned as a result of an increase in volume due to favourable business conditions caused by the impact of network security failures impacting other businesses, loss of market, or any other consequential loss.
Business services	means software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), network as a service (NaaS), voice over internet protocol, and telephony services that: 1. you use regularly in the normal course of your business; 2. you are charged a fee for on a regular periodic basis, no less frequently than on a semi-annual basis; and 3. are provided to you pursuant to a written contract.
Claim	means: 1. a written demand for money or services including the service of a suit or institution of arbitration proceedings; 2. with respect to coverage provided under Section II.B, REGULATORY DEFENCE AND PENALTIES, a regulatory proceeding; 3. with respect to coverage under Section II.C, PCI FINES AND ASSESSMENTS, a written demand for PCI fines and assessments; and 4. a written request to toll or waive a statute of limitations applicable to a potential claim described in paragraph 1. above. All claims that have a common nexus of fact, circumstance, situation, event, transaction, or cause, or a series of related facts, circumstances, situations, events, transactions, or causes will be considered a single claim made against you on the date the first such claim was made.
Claim expenses	means: 1. reasonable fees charged by legal counsel to which we have agreed to defend a claim; and 2. all other fees, costs, and charges for the investigation, defence, and appeal of a claim, if incurred by us or by you with our prior written consent (which we will not unreasonably withhold); and 3. premiums on appeal bonds, provided that we will not be obligated to apply for or furnish such appeal bonds. Claim expenses do not include salary, charges, wages, or expenses of any senior executive or employee, or costs to comply with any court or regulatory orders, settlements, or judgments.

Computer replacement costs	means the reasonable costs you incur, with our prior written consent (which we will not unreasonably withhold), to restore or replace computer hardware or tangible equipment owned or leased by you impacted by a loss of firmware integrity resulting from a security failure .
Computer systems	means: 1. computers and related peripheral components, including Internet of Things (IoT) devices; 2. systems and applications software; 3. terminal devices; 4. related communications networks; 5. mobile devices (handheld and other wireless computing devices); and 6. storage and back-up devices by which electronic data is collected, transmitted, processed, stored, backed up, retrieved, and operated by you on your own behalf. Computer systems include hosted computer systems.
Consumer redress awards	means any monetary amounts you are legally obligated or have agreed to deposit into a consumer redress fund as equitable relief for the payment of consumer claims due to an adverse judgement determination or settlement of a regulatory proceeding . Consumer redress awards do not include any sums paid which constitute taxes, fines, penalties, injunctions, or sanctions.
Contingent business interruption loss	means: 1. the net profit that would have been earned before taxes on income, or net loss that would not have been incurred, directly due to the partial or complete interruption of hosted computer systems; and 2. continuing normal operating expenses (including payroll), but only to the extent that such operating expenses must reasonably continue during the indemnity period. Provided, however, that contingent business interruption loss will not include net profit that would likely have been earned as a result of an increase in volume due to favourable business conditions caused by the impact of network security failures impacting other businesses, loss of market, or any other consequential loss.
Continuity date	means the date specified in Item 11. of the Declarations. Provided, if a subsidiary is acquired during the policy period , the continuity date for such subsidiary will be the date the named insured acquired such subsidiary .
Court attendance costs	means the reasonable costs (including the salaries of employees) and expenses of attending at our request a trial, hearing, deposition, mediation, arbitration, or other proceeding relating to the defence of any claim .
Criminal reward costs	means any amount offered and paid by us , acting reasonably, for information that leads to the arrest and conviction of any individual(s) committing or trying to commit any illegal act related to any coverage under this Policy. This Policy will not cover amounts offered and paid-for-information provided by you , your legal counsel and/or auditors, whether internal or external, individuals hired or retained in response to the aforementioned illegal acts, or other individuals with responsibilities for supervision or management of the aforementioned individuals and entities.
Crisis management costs	means the following reasonable fees or expenses agreed to in advance by us, acting reasonably, to mitigate covered damages, loss, claim expenses, breach response costs, or breach response services due to a public relations event: 1. a public relations or crisis management consultant; 2. media purchasing, or for printing or mailing materials intended to inform the general public about the public relations event;

	3. providing notifications to individuals where such notifications are not required by breach notice law, including notices to your non-affected customers, employees, or clients; and 4. other costs approved in advance by us. If you do not obtain our agreement to incur the reasonable fees or expenses, we will pay for fees and expenses incurred up to the amount we would have authorised had you asked us first.
Cyber extortion	means any: 1. threat made by an individual or organisation against you expressing the intent to: a. transfer, pay, or deliver any funds or property belonging to you, or held by you on behalf of others, using computer systems without your permission, authorisation, or consent; b. access, acquire, sell, or disclose non-public information in your care, custody, or control, provided such information is stored in an electronic medium in computer systems and is retrievable in a perceivable form; c. alter, damage, or destroy any computer program, software, or other electronic data that is stored within computer systems; d. maliciously or fraudulently introduce malicious code or ransomware into computer systems; or e. initiate a denial of service attack on computer systems; or 2. introduction of malicious code or ransomware into computer systems by an individual or organisation; or, 3. denial of service attack on computer systems; where such threat is made or act is committed for the purpose of demanding payment of money, securities, Bitcoin or other virtual currencies, property, or goods from you.
Cyber extortion expenses	means the following reasonable and necessary costs incurred with our prior written consent(which we will not unreasonably withhold): 1. money, securities, Bitcoin, or other virtual currencies paid at the direction and demand of any individual or organisation committing cyber extortion and costs incurred solely in, and directly from, the process of making or attempting to make such a payment; 2. value of property or goods demanded by any individual or organisation committing cyber extortion and costs incurred solely in, and directly from, the process of delivering or attempting to deliver to such property or goods; and 3. reasonable and necessary costs, fees, and expenses to respond to a cyber extortion. The value of cyber extortion expenses will be determined as of the date such cyber extortion expenses are paid.
Cyber operation	means the use of a computer system by, on behalf of, at the direction, or under the control of a sovereign state to disrupt, deny, degrade, manipulate or destroy information in a computer system of or in another sovereign state. For the purpose of the definition of cyber operation only, computer system means any computers and related peripheral components (including Internet of Things (IoT) devices), systems and applications software, terminal devices, related communications networks, mobile devices (handheld and other wireless computing devices), and storage and back-up devices.

Damages	means a monetary judgement or award that you are legally obligated to pay, including pre-judgment and post-judgment interest, or settlement agreed to by you and us. Damages does not mean the following: 1. future profits, restitution, disgorgement of profits, or unjust enrichment, or the costs of complying with orders granting injunctive or equitable relief; 2. return or offset of fees, charges, or commissions charged by or owed to you for goods or services already provided or contracted to be provided; 3. funds transfer liability loss; 4. costs incurred by you to correct, re-perform, or complete any service, including any technology services or professional services; 5. liquidated damages, contractual service credits or penalties, but only to the extent such liquidated damages, contractual service credits or penalties exceed the amount for which the insured would have been liable in the absence of any agreement to pay such liquidated damages, contractual service credits or penalties; 6. civil or criminal fines or penalties, civil or criminal sanctions, payroll or other taxes, or loss of tax benefits, or amounts or relief uninsurable under applicable law; 7. any damages which are a multiple of compensatory damages, or punitive or exemplary damages, unless insurable by law in any applicable jurisdiction that most favours coverage for such punitive or exemplary damages; 8. discounts, coupons, prizes, awards, or other incentives offered by you; 9. fines, costs, assessments, or other amounts you are responsible to pay under a merchant service agreement; 10. any amounts for which you are not liable, or for which there is no legal recourse against you; or 11. royalty or licensing fees.
Data breach	means the unauthorised access to, unauthorised disclosure of or loss of personally identifiable information or third party corporate information including resulting from a security failure.
Denial of service attack	means a deliberate or malicious attack that makes computer systems unavailable to its intended users, temporarily or indefinitely disrupting the services of a host that you use by directing an excessive volume of electronic data to that host.
Digital asset	means any of your electronic data or computer software. Digital assets do not include computer hardware of any kind.
Employee	means any past, present, or future: 1. person employed by the named insured or subsidiary as a permanent, part-time, seasonal, leased, or temporary employee, intern, or any volunteer; and 2. senior executive; but only while acting on behalf of the named insured or subsidiary and in the scope of the duties of their role and business operations of the named insured or subsidiary.
Essential Service	Means a service that is essential for the maintenance of vital functions of a sovereign state including but not limited to financial institutions and associated financial market infrastructure, health services or utility services.
Event	means a funds transfer liability, incident, privacy liability, technology and professional services wrongful act, or multimedia wrongful act. All events that have a common nexus of fact, circumstance, situation, transaction, or cause, or a series of related facts, circumstances, situations, transactions, or causes will be considered a single event occurring on the date the first such event occurred.

Extra expenses	means your reasonable and necessary additional costs incurred to avoid or minimise a business interruption loss, including: 1. the reasonable and necessary additional costs of sourcing your products or services from alternative sources in order to meet contractual obligations to supply your customers and clients; 2. the reasonable and necessary additional costs of employing contract staff or overtime costs for employees, including your internal IT department, in order to continue your business operations which would otherwise have been handled in whole or in part by computer systems or service provider; and 3. the reasonable and necessary additional costs of employing specialist consultants, including IT forensic consultants, in order to diagnose and fix a security failure or systems failure. Provided, however, that such additional costs do not exceed the amount of loss that otherwise would have been payable as business interruption loss. Extra expenses does not mean and will not include: 1. costs incurred to update, restore, replace, upgrade, maintain, or improve computer systems: a. to a level greater than existed before a security failure, unless the costs to upgrade to a more current or secure version of functionally equivalent components of computer systems is no more than 25% greater than the costs that would have been incurred to repair or replace computer systems that existed before a security failure; or b. to a level greater than existed before a system failure; or 2. costs incurred to acquire or install computer systems which did not form a part of computer systems immediately prior to the security failure or system failure.
Funds transfer fraud	means a fraudulent instruction transmitted by electronic means, including through social engineering, to you or your financial institution including a trust account provider directing you, or the financial institution including a trust account provider: 1. to debit, or instruct to authorise to debit, an account for which the named insured or subsidiary is an authorised custodian, and to transfer, pay, or deliver money or securities from such account; or 2. to debit, or instruct to authorise to debit, an account held by the named insured or subsidiary, or held by the named insured or subsidiary on behalf of a third party, and to transfer, pay, or deliver money or securities from such account; or 3. to transfer or deliver tangible property owned or held by the named insured or subsidiary; which purports to have been transmitted by you or your vendors, business partners, or existing clients, and impersonates such party including through the use of deepfakes, but was transmitted by someone other than you or your vendors, business partners, or existing clients, and without such party's knowledge or consent. The "financial institution" does not include any such entity, institution, or organisation that is an insured.
Funds transfer liability	means distribution of fraudulent wire transfer or payment instructions which instruction purports to have been transmitted by you directing your vendors, business partners, or existing clients to transfer funds to a third party, but was transmitted by someone other than you as the result of a security failure.
Funds transfer liability loss	means a monetary judgement or award that you are legally obligated to pay, or a settlement agreed to by you and us, because of the transfer of money or securities, or digital currencies by any of your vendors, business partners, or existing clients to a third party as the direct result of a funds transfer liability.

Funds transfer loss	means: 1. loss of money, securities, digital currencies, or tangible property directly resulting from funds transfer fraud or personal funds fraud; and 2. reasonable and necessary costs, fees, and expenses to respond to funds transfer fraud or personal funds fraud. Funds transfer loss does not mean and will not include: a. the loss of personal money, securities, or property of your employees with the exception of senior executives. b. chargeback loss arising from the acceptance payment cards used fraudulently.
Hosted computer systems	means: 1. computers and related peripheral components, including Internet of Things (IoT) devices; 2. systems and applications software; 3. terminal devices; 4. related communications networks; 5. mobile devices (handheld and other wireless computing devices); and 6. storage and back-up devices by which electronic data is collected, transmitted, processed, stored, backed up, retrieved, and operated by a third party vendor, but only for providing hosted computer services, including SaaS, IaaS, NaaS and PaaS, to you pursuant to a written contract.
Impacted State	means a sovereign state where a cyber operation has had a major detrimental impact on: 1. the functioning of that sovereign state due to disruption to the availability, integrity or delivery of an essential service in that sovereign state; and/or 2. the security or defence of that sovereign state.
Impersonation fraud	means fraudulent electronic communications or websites designed to impersonate you or any of your products provided that such fraudulent communications or websites do not arise out of or result from any security failure.
Impersonation repair costs	means: 1. the cost of retaining a law firm and public relations firm incurred by you to create and publish a press release or establish a website to advise your customers and prospective customers of an impersonation fraud; and 2. the cost of reimbursing your existing customers for their loss of money or tangible property directly resulting from an impersonation fraud; and 3. the cost of retaining a third party for the removal of websites designed to impersonate you.
Incident	means adverse publication, cyber extortion, data breach, funds transfer fraud, impersonation fraud, invoice manipulation, personal funds fraud, public relations event, security failure, or systems failure. All incidents that have a common nexus of fact, circumstance, situation, event, transaction, or cause, or series of related facts, circumstances, situations, events, transactions, or causes will be considered a single incident occurring on the date the first such incident occurred.

Indemnity period	means the time period that: 1. begins on the date and time that the partial or complete interruption of computer systems first occurred; and 2. ends on the earlier of the date and time that the interruption to your business operations resulting from such interruption of computer systems: (i) ends; or (ii) could have ended if you had acted with due diligence and dispatch. However, in no event will the indemnity period exceed 365 days.
Insured, you, or your	means: 1. the named insured; 2. a subsidiary; 3. senior executives and employees; 4. an independent contractor, who is a natural person, solely acting in the normal course of the named insured or subsidiary's business operations while under their direct supervision; 5. with respect to Sections II.A, NETWORK AND INFORMATION SECURITY LIABILITY, II.B, REGULATORY DEFENCE AND PENALTIES, and II.E, TECHNOLOGY ERRORS AND OMISSIONS, any person or entity you have agreed in a written contract or agreement to add as an additional insured to a policy providing the type of coverage afforded by this Policy, provided such contract or agreement is in effect or becomes effective during the policy period, and solely for such person's or entity's liability arising out of the named insured's or subsidiary's acts (hereafter an additional insured); 6. the estates, heirs, legal representatives, or assignees of any employee or senior executive in the event of their death, incapacity, insolvency, or bankruptcy but solely for the estates', heirs', legal representatives', or assignee's liability arising out of the acts committed by the employee or senior executive, in their capacity as such; and 7. the spouse, domestic partner, or civil partner of any employee or senior executive solely for such spouse's, domestic partner's, or civil partner's liability resulting from a claim against the employee or senior executive, in their capacity as such; or their ownership or interest in property which the claimant seeks as recovery for a claim against the employee or senior executive, in their capacity as such.
Invoice Manipulation	means the release or distribution of any fraudulent invoice or payment instruction to a third party as a direct result of a security failure.
Invoice Manipulation Loss	means your direct net costs, excluding any profit, to provide goods, products, or services to a third party for which you are unable to collect payment after transfer of such goods, products, or services to a third party as the direct result of invoice manipulation.
Loss	means business interruption loss, computer replacement costs, contingent business interruption loss, court attendance costs, criminal reward costs, crisis management costs, cyber extortion expenses, extra expenses, funds transfer loss, impersonation repair costs, invoice manipulation loss, proof of loss preparation expenses, reputational harm loss, service fraud loss, and restoration costs.
Malicious code	means any type of malicious, unauthorised, corrupting or harmful software program, code, or script specifically designed to create system vulnerabilities and destroy, alter, steal, contaminate, or degrade the integrity, quality, or performance of: 1. electronic data used or stored in any computer system or network; or 2. a computer network, any computer application software, or computer operating system or related network.

Media content	means content in any form, regardless of its nature or medium, including any data, text, sounds, numbers, images, graphics, videos, streaming content, webcasts, podcasts, or blogs. Media content does not include any biometric personally identifiable information computer software or the actual goods, products, or services described, referenced, illustrated, or displayed in such media content .
Merchant service agreement	means any agreement between you and a financial institution, payment card company, payment card processor, or independent service operator, that enables you to accept credit cards, debit cards, prepaid cards, or other payment cards for payments or donations.
Multimedia wrongful act	means any of the following actually or allegedly committed by you in the normal course of your business in communicating, reproducing, publishing, disseminating, displaying, releasing, transmitting, or disclosing media content , including social media authorised by you : 1. defamation, libel, slander, trade libel, infliction of emotional distress, outrage, outrageous conduct, or other tort related to disparagement or harm to the reputation or character of any person or organisation; 2. violation of the rights of privacy of an individual, including false light and public disclosure of private facts; 3. invasion or interference with an individual's right of publicity, including commercial appropriation of name, persona, voice, or likeness; 4. plagiarism, piracy, or misappropriation of ideas under implied contract; 5. infringement of copyright, domain name, trademark, trade name, trade dress, logo, title, metatag, slogan, service mark, or service name; or 6. improper deep-linking or framing within electronic content.
Named insured	means the individual, partnership, entity, or corporation designated as such in Item 1. of the Declarations, or by endorsement to this Policy.
Panel Providers	means those firms listed on our web site at http://www.coalitioninc.com/au/panel
PCI fines and assessments	means the direct monetary fines and assessments for fraud recovery, operational expenses including card reissuance fees and notification of cardholders, and case management fees owed by you under the terms of a merchant service agreement , but only where such fines or assessments result from a data breach . PCI fines and assessments will not include any charge backs, interchange fees, discount fees, or other services related fees, rates, or charges.
Personal funds fraud	means the loss of personal money, securities, or property from a personal bank account of a senior executive as a direct result of a security failure of the named insured's or a subsidiary's computer systems .
Personally identifiable information	means any information about an identified individual, or an individual who is reasonably identifiable, whether true or not, and whether recorded in a material form or not, or otherwise that is required by any federal, provincial, territorial, state, local, or foreign law or regulation to be protected from unauthorised access, acquisition, or public disclosure.
Policy period	means the period of time between the inception date shown in the Declarations and the effective date of termination, expiration, or cancellation of this Policy and specifically excludes any Optional Extended Reporting Period.

Pollutants	means any solid, liquid, gaseous, or thermal irritant or contaminant exhibiting hazardous characteristics as is or may be identified on any list of toxic or hazardous substances pursuant to, any governmental, federal, provincial, territorial, state, local, or foreign legislation or agency, including gas, acids, alkalis, chemicals, odours, noise, lead, petroleum or petroleum-containing products, heat, smoke, vapour, soot, fumes, radiation, asbestos or asbestos-containing products, waste (including material to be recycled, reconditioned, or reclaimed), electric, magnetic, or electromagnetic field of any frequency, as well as any air emission, wastewater, sewage, infectious medical waste, nuclear materials, nuclear waste, mould, mildew, fungus, bacterial matter, mycotoxins, spores, scents or by-products and any non-fungal micro-organism, or non-fungal colony form organism that causes infection or disease.
Privacy liability	means: 1. your actual or alleged failure to timely disclose a security failure or data breach resulting in a violation of any breach notice law; 2. your failure to comply with those provisions in your privacy policy that: a. mandate procedures to prevent the loss of personally identifiable information; b. prohibit or restrict disclosure, sharing, or selling of an individual's personally identifiable information; or c. require you to give access to personally identifiable information or to amend or change personally identifiable information after a request is made by the concerning individual; provided that no senior executive knew of or had reason to know of any such conduct; and failure to administer an identity theft prevention program or an information program pursuant to any governmental, federal, provincial, territorial, or state
Privacy policy	means any public written statements that set forth your policies, standards, and procedures for the collection, use, disclosure, sharing, dissemination, and correction or supplementation of, and access to, personally identifiable information .
Professional services	means those services specified in Item 7. of the Declarations and performed by the named insured or a subsidiary for others' benefit pursuant to a written contract.
Proof of loss preparation expenses	means the reasonable and necessary costs you incur with our prior written consent (which we will not unreasonably withhold) for a third party forensic accounting firm to assist you with preparing a proof of loss as required by Section V. CLAIMS PROCESSES, PROOF OF LOSS with respect to business interruption loss, contingent business interruption loss, extra expenses or reputational harm loss covered under this Policy.
Public relations event	means: 1. the publication or imminent publication in a newspaper (or other general circulation print publication), on radio or television, or electronic news website (but not including social media) of a security failure or data breach that has resulted in a covered claim under this Policy; and 2. a security failure or data breach that results in covered breach response costs under this Policy or which reasonably may result in a covered claim under the Policy.
Ransomware	means any malicious code designated to block your access to computer systems or digital assets , delete or otherwise harm your computer systems or digital assets , or cause a security failure , until a sum of money is paid.

Regulatory penalties	means monetary fines and penalties, including consumer redress awards, imposed in a regulatory proceeding to the extent insurable under applicable law. Regulatory penalties will not mean any: 1. costs to comply with injunctive relief; 2. costs to establish or improve privacy or security practices; or 3. audit, reporting, or compliance costs.
Regulatory proceeding	means a request for information, civil investigative demand, or civil proceeding commenced by service of a complaint or similar proceeding brought by or on behalf of the Office of the Australian Information Commissioner, Australian Securities & Investments Commission, U.S. regulator Security and Exchange Commission (SEC) only from Regulation S-P (17 C.F.R. § 248), or any other domestic or foreign governmental entity including any federal, provincial, territorial, state or local entity in such entity's regulatory or official capacity, in connection with such proceeding arising from a security failure or data breach. Other than the foregoing, regulatory proceeding does not include a request for information, civil investigative demand, or civil proceeding commenced by service of a complaint or similar proceeding brought by the Securities and Exchange Commission (SEC) and similar federal, state, local, or foreign governmental entities.
Reputational harm loss	means the net profit that would have been earned before taxes on income, or net loss that would not have been incurred solely and directly as the result of any adverse publication. Reputational harm loss does not include any: 1. costs to rehabilitate your reputation, including legal costs or expenses; 2. breach response costs, crisis management costs, business interruption loss, contingent business interruption loss, or extra expenses; 3. Costs not directly caused by an adverse publication. Reputational harm loss will not include net profit that would likely have been earned before taxes on income as a result of an increase in volume due to favourable business conditions caused by the impact of security failures, data breaches, cyber extortion, or privacy liability impacting other businesses, loss of market, or any other consequential loss. Further, due consideration will be given to the following when calculating reputational harm loss: 1. the experience of your business before the adverse publication and probable experience thereafter during the reputation indemnity period had there been no adverse publication and to the continuation of normal charges and expenses that would have existed had no adverse publication occurred; and expenses that would have existed had no adverse publication occurred; and 2. any reputational harm loss made up or recovered during, or within a reasonable time after the end of, the reputation indemnity period.
Reputation indemnity period	means the one hundred and eighty (180) day period that begins at the conclusion of the reputation waiting period.
Reputation waiting period	means the amount of time set forth in Item 5.O. of the Declarations that must elapse after the date upon which the adverse publication was first published. The reputation waiting period cannot be insured.

Restoration costs	means: - the reasonable and necessary costs you incur to replace, restore, or recreate digital assets to the level or condition at which they existed prior to a security failure or systems failure; or - the cost for the most current version of digital assets if it is substantially equivalent to (or less than) the original cost of digital assets; if such digital assets cannot be replaced, restored, or recreated, then restoration costs will be limited to the actual, reasonable, and necessary costs you incur to reach this determination. Restoration costs does not mean and will not include: - any costs or expenses incurred to identify, remove, or remediate computer program errors or vulnerabilities; - the economic or market value of any digital assets, including trade secrets, or the costs to re-perform any work product contained within any digital assets; or - costs incurred to acquire or install digital assets which did not exist immediately prior to the security failure or systems failure.
Retroactive date	means the date specified in Item 10. of the Declarations.
Security failure	means the failure of security of computer systems which results in: - loss, alteration, corruption, or damage to software, applications, or electronic data existing in computer systems; - transmission of malicious code from computer systems to third party computer systems that are not owned, operated, or controlled by the named insured or subsidiary; or - a denial of service attack on the named insured's or subsidiary's computer systems; or - access to or use of computer systems in a manner that is not authorised by you, including when resulting from the theft of a password. Security failure does not mean and will not include any failure of computers, related peripheral components, or mobile devices that are owned or leased by an employee and not used for the business operations of the named insured or subsidiary.
Senior executive	means any partner, principal, director, executive board member, in-house counsel, risk manager, chief information officer, chief information security officer, chief privacy officer, chief financial officer, chief executive officer, chief operating officer, or functional equivalent, but only while acting on your behalf in the scope of your business operations.
Service fraud loss	means direct financial loss that you incur as the result of being charged a fee for the fraudulent use of business services , including fraudulent use arising from cryptojacking.
Service provider	means any third party that is responsible for the processing, maintenance, protection, or storage of digital assets pursuant to a written contract.
Submission	means all applications and proposal forms, including any attachments thereto and supplemental information, submitted by or on behalf of the named insured to us in connection with the request for or underwriting of this Policy, or any prior policy issued by us of which this Policy is a renewal.
Subsequent Legislation	means: - An act or regulation as amended, replaced or re-enacted; or - where an act or regulation has been repealed, the current equivalent act or regulation (Commonwealth, State or Territory) with materially the same object or purpose whether in whole or in part

Subsidiary	means any organisation in which the named insured: - owns or controls either directly or indirectly 50% on or before the inception date of this Policy, or more of the outstanding voting stock or shareholder voting power or has the right to elect or appoint the majority of the board of directors or persons to an equivalent executive management function; and - has recognised the revenues in the submission for this Policy. An organisation ceases to be a subsidiary on the date, during the policy period, that the named insured ceases to own or control, directly or indirectly, 50% or more of the outstanding voting or shareholder voting power, or ceases to control the right to elect or appoint the majority of the board of directors or persons to equivalent executive management functions. The named insured will give written notice to us of any acquisition or creation of an organisation with ownership interest greater than 50%, no later than sixty (60) days after the effective date of such acquisition or creation. Automatic coverage of such organisation is granted until the end of the policy period subject to the following criteria: - the newly created or acquired organisation has substantially similar business operations; - the new organisation's gross revenue is equal to or less than 10% of the total gross revenue the named insured has listed on the submission for this Policy; and - prior to the effective date of such acquisition or creation, no senior executive of the named insured or of the acquired or created organisation, knew or could have reasonably expected that a claim would be made or coverage triggered under any Insuring Agreement in Section II, WHAT WE COVER. Where such acquisition or creation does not qualify for the automatic coverage described above, no coverage is granted and such acquired or created organisation is not included under this Policy unless and until agreed by us in writing. Upon receipt of notice of such acquisition or creation, we may, at our sole option, agree to appropriately endorse this Policy subject to additional premium and/or change terms and conditions.
Systems failure	means any: - unintentional, unplanned, or unexpected computer systems disruption, damage, or failure where the proximate cause is not a security failure, loss of or damage to any physical equipment or property, or planned or scheduled outage or maintenance of computer systems or a third party's computer systems (including downtime that is the result of a planned outage lasting longer than initially expected); or - disruption or voluntary shutdown of computer systems by you, with our prior consent (which we will not unreasonably withhold), in order to mitigate covered loss under this Policy. Systems failure does not include any: - failure of hosted computer systems that results in an outage that extends beyond the services being provided to you by hosted computer systems; - suspension, cancellation, revocation, or failure to renew any domain names or uniform resource locators; - failure to adequately anticipate or capacity plan for normal and above operational demand for computer systems except where this demand is a denial of service attack; - failure of any computer hardware that has been declared as end-of-life by the original equipment manufacturer; - design failure or manufacturing defect in third party computer

	software or computer hardware.
Tangible property	means items or objects that can be felt or touched. Tangible property does not include: 1. digital assets; 2. any form of intellectual property, including trade secrets; or 3. money, securities or digital currencies. The value of any covered tangible property will be the cost to replace such tangible property with property of comparable material and quality. The replacement cost value for any tangible property does not include any profit or mark-up you are unable to collect as a result of the loss of tangible property.
Technology and professional services wrongful act	means: 1. any actual or alleged error, omission, misstatement, neglect, or unintentional breach of duty or written contract, by you or any person for whose actual or alleged error, omission, neglect or unintentional breach of duty or written contract the named insured or subsidiary is legally liable for, in rendering technology services or professional services; or 2. any actual or alleged act, error, omission, misstatement, neglect, or unintentional breach of contract, by you or any person for whose actual or alleged error, omission, misstatement, neglect or unintentional breach of written contract the named insured or subsidiary is legally liable for, that results in the failure of technology products to perform as intended.
Technology products	means computer or telecommunications hardware or software products, or related components or products, that are created, manufactured, developed, sold, or distributed by the named insured or subsidiary for others' benefit pursuant to written contract for a fee, including software updates, service packs, and other maintenance releases for such products.
Technology services	means computer and electronic technology services, including data backup and processing, Internet and mobile services, email services, SaaS, PaaS, IaaS, NaaS, data and application hosting, computer systems analysis, technology and security consulting and training, custom software programming for a specific customer, computer and software systems installation and integration, computer and software support, and network management services, performed by the named insured or subsidiary for others' benefit pursuant to a written contract for a fee.
Third party corporate information	means any information of a third party held by you which is not available to the general public and is provided to you subject to a mutually executed written confidentiality agreement between you and the third party or which you are legally required to maintain in confidence. However, third party corporate information does not include personally identifiable information .
War	means the use of physical force by a sovereign state against another sovereign state, or as part of a civil war, rebellion, revolution, insurrection, or military or usurped power, whether war be declared or not.
Waiting period	means the number of hours set forth in Item 5.K. of the Declarations.
We, us, or our	means the insurers of this Policy.