AVIVA

Your Sample Cyber Insurance Policy Wording

Please keep this document safe and refer to it if you need to make a claim.

If you need this document in an alternative format, please speak to your insurance adviser.

Policy Introduction for Policy Number

Welcome to Aviva. We are committed to providing a first-class service. Aviva has the experience and longevity of a company who can trace its roots back to the establishment of the Hand in Hand Fire & Life Insurance Society in London in 1696.

This is your Cyber Insurance policy which sets out your insurance protection in detail.

Your premium has been calculated on the basis of the extent of cover you have selected which is specified in The Schedule, the information you have provided and the declaration you have made. Please read the policy and The Schedule carefully to ensure that the cover meets your requirements.

Please contact your insurance adviser if you have any questions or if you wish to make adjustments.

Contents

This policy consists of individual sections. You should read this policy in conjunction with The Schedule which confirms the sections you are insured under and gives precise details of the extent of your insurance protection

The Contract of Insurance

The contract of insurance between you and us consists of the following elements, which must be read together:

- your policy wording;
- the information provided by You and/or the application form;
- the information contained on your Statement of Fact issued by Us;
- the policy schedule;
- any notice issued by Us at renewal;
- any endorsement to your policy; and
- the information under the heading 'Important Information' which We give You when You take out or renew your policy

In return for You having paid or agreed to pay the premium, We will provide the cover set out in this policy, to the extent of and subject to the terms contained in or endorsed on this policy.

Breach of term

We agree that where there has been a breach of any term (express or implied) which would otherwise result in us automatically being discharged from any liability, then such a breach shall result in any liability we might have under this policy being suspended. Such a suspension will apply only from the date and time at which the breach occurred and up until the date and time at which the breach is remedied. This means that we will have no liability in respect of any loss occurring, or attributable to something happening, during the period of suspension.

Terms not relevant to the actual loss

Where there has been non-compliance with any term (express or implied) of this policy, other than a term that defines the risk as a whole, and compliance with such term would tend to reduce the risk of:

- loss of a particular kind, and/or
- loss at a particular location, and/or
- loss at a particular time,

then we agree that we may not rely on the non-compliance to exclude, limit or discharge our liability under this policy if you show that non-compliance with the term could not have increased the risk of the loss which actually occurred in the circumstances which it occurred.

Choice of Law

The appropriate law as set out below will apply unless you and the insurer agree otherwise:

- The law applying in that part of the UK, the Channel Islands or the Isle of Man in which you normally live or (if applicable) the first named policyholder normally lives, or
- In the case of a business, the law applying in that part of the UK, the Channel Islands or the Isle of Man where it has its principal place of business, or
- Should neither of the above be applicable, the law of England and Wales will apply.

Use of Language

All communications relating to this contract will be in English.

Making a Claim

Should you need to make a claim under this policy, please contact us on:

0800 051 4473

In all cases, please quote your policy number.

Calls to 0800 numbers from UK landlines and mobiles are free. For our joint protection telephone calls may be recorded and/or monitored.

Financial Services Compensation Scheme

Depending on the circumstances of your claim you may be entitled to compensation from the Financial Services Compensation Scheme (FSCS) if we cannot meet our obligations. See **fscs.org.uk**

Complaints Procedure

What to do if you are unhappy

If you are unhappy with any aspect of the handling of your insurance Aviva would encourage you, in the first instance, to seek resolution by contacting your insurance advisor. Contact details can be found on your insurance documents.

What will happen if you complain

If your complaint is not resolved quickly:

- Your complaint will be acknowledged promptly.
- A dedicated complaint expert will be assigned to review your complaint.
- A thorough and impartial investigation will be carried out.
- You will be kept updated of the progress.
- Everything will be done to resolve things as quickly as possible.
- A written response will be sent to you within eight weeks of receiving your complaint, this will inform you of the results of the investigation or explain why this isn't possible.

Where your concerns are unable to be resolved or have not been resolved within eight weeks, you may be able to ask the Financial Ombudsman Service (FOS) to carry out an independent review. Whilst firms are bound by their decision you are not. Contacting them will not affect your legal rights.

The Insured can contact the **FOS** on **0800 023 4567** or visit their website at **www.financial-ombudsman.org.uk**, where you will find further information.

Cyber

Section 1: Cyber Incident Response Costs

Cover A: Crisis Management

Where a Cyber Incident, which directly affects You or an Outsourced Service Provider, has been first discovered during the Period of Insurance, We will cover You for the resulting reasonable cost of:

(1) accessing Our Cyber Incident Crisis Manager via Our 24/7 hotline

(2) Engaging Our Cyber Incident Crisis Manager to provide expert advice and consultancy, and to coordinate and oversee the full response to the Cyber Incident.

Cover B: IT Investigation and Forensic Costs

Where a Cyber Incident, which directly affects You or an Outsourced Service Provider, has been first discovered during the Period of Insurance, We will cover You for the resulting reasonable cost of specialist external IT consultants to:

(1) investigate whether a Cyber Incident has occurred

(2) conduct a forensic investigation to determine the root cause, and stop or contain the Cyber Incident

(3) determine whether any Data has been lost, stolen, accessed, or disclosed as a result of the Cyber Incident

(4) certify that Your Computer Equipment is compliant with PCI-DSS, where the Cyber Incident affects payment card data

Cover C: Legal and Regulatory Costs

Where a Cyber Incident, which directly affects You or an Outsourced Service Provider, has been first discovered during the Period of Insurance, We will cover You for the resulting reasonable cost of external legal advice to:

(1) manage Your legal response to the Cyber Incident

(2) draft Data Security Breach notifications

(3) notify the Cyber Incident to any appropriate governmental, regulatory, law enforcement, professional or statutory body

Cover D: Communication Costs

Where a Cyber Incident, which directly affects You or an Outsourced Service Provider, has been first discovered during the Period of Insurance, We will cover You for the resulting reasonable cost of public relations consultants to:

(1) provide advice to minimise adverse publicity

(2) create a communication plan for internal and external stakeholders

(3) provide media training to relevant Employees

(4) issue statements via Your website, email and social media accounts

(5) manage and monitor Your social media accounts

Cover E: Privacy Breach Management Costs

Where a Cyber Incident, which directly affects You or an Outsourced Service Provider, has been first discovered during the Period of Insurance, We will cover You for the resulting reasonable cost of:

(1) notifying any Data Subject potentially affected by the Cyber Incident

(2) providing a credit monitoring, credit protection or identity fraud remediation service to the affected Data Subjects

(3) setting up a telephone help line to assist Data Subjects after they have been notified of the Cyber Incident

We will also cover You for under (1), (2), and (3) above where You have contractually agreed to indemnify a third party against such costs resulting from the Cyber Incident.

Cover F: Extortion Resolution Costs

Where a Cyber Extortion, made against You, has been first discovered during the Period of Insurance, We will cover You for the resulting reasonable and necessary cost of:

(1) appointing a consultant to advise You, undertake relevant threat intelligence and due diligence, and handle the negotiation of the Cyber Extortion

(2) a Cyber Extortion Payment

(3) a Cyber Extortion Payment which is stolen before reaching the Cyber Extortionist

provided that it is legally permissible to reimburse any such Cyber Extortion Payment

Cover G: Criminal Reward Fund

We will provide cover to You for a Reward where You have suffered loss arising from a Cyber Incident or Cyber Crime provided We determine that it is legally permissible to reimburse any such Reward.

Cover H: Resilience Improvement Costs

Where a Cyber Incident, which directly affects You, has been first discovered during the Period of Insurance, We will cover You for the resulting reasonable cost of:

(1) Our Cyber Incident Crisis Manager reviewing the findings within any post-event report

(2) Our Cyber Incident Crisis Manager or providing an action plan to improve the resilience of Your Computer Equipment

(3) implementing items recommended by Our Cyber Incident Crisis Manager or for which are necessary to improve the resilience of Your Computer Equipment to prevent a similar future Cyber Incident.

Section 2: Computer and Data Rectification Costs

Cover A: Data Restoration Costs

Where a Cyber Incident, which directly affects You or any Outsourced Service Provider, has been first discovered during the Period of Insurance, We will cover You for the resulting reasonable and necessary cost of

(1) reinstating, recreating or restoring Your Data within Your Computer Equipment

(2) locating and removing a detectable Virus or Similar Mechanism contained in any of Your Computer Equipment

(3) re-licensing software that has been irreparably damaged by the Cyber Incident

Cover B: Hardware Replacement (Bricking) Costs

Where a Cyber Incident, which directly affects You, has been first discovered during the Period of Insurance, We will cover You for the resulting reasonable and necessary cost of replacing any of Your physical Computer Equipment that has been damaged as a result of the Cyber Incident.

Exceptions

The following Exception applies to Section 2, Cover B, Hardware Replacement (Bricking) Costs in addition to the Policy Exceptions.

Operational Technology

We will not provide cover for any replacement of industrial control systems and any information technology to steer or control technical processes, any embedded systems or any other industrial information technology, including operational technology.

Section 3: Business Interruption

Cover A: Loss of Profit and Increased Costs of Working – Cyber Incident

We will cover You for any Loss of Profit and/or Increased Costs of Working sustained during the Indemnity Period and directly caused by a Cyber Incident which:

(a) is first discovered during the Period of Insurance, and

(b) directly affects Your Computer Equipment or Data held within Your Computer Equipment

including where such loss arises from a necessary voluntary and intentional shutdown of Your Computer Equipment initiated by You to mitigate and contain the Cyber Incident, provided that such Cyber Incident lasts longer than the Waiting Period

Cover B: Loss of Profit and Increased Costs of Working – System Failure

We will cover You for any Loss of Profit and/or Increased Costs of Working sustained during the Indemnity Period and directly caused by a System Failure which

(a) is first discovered during the Period of Insurance, and

(b) directly affects Your Computer Equipment or Data held within Your Computer Equipment.

provided that such System Failure lasts longer than the Waiting Period

Cover C: Loss of Profits and Increased Costs of Working – Outsourced Service Provider

We will cover You for any Loss of Profit and/or Increased Costs of Working sustained during the Indemnity Period and directly caused by a Cyber Incident or System Failure directly affecting the Computer Equipment of an Outsourced Service Provider which:

(a) is first discovered during the Period of Insurance, and

(b) directly affects your Data

provided that such Cyber Incident or System Failure lasts longer than the Waiting Period

Cover D: Additional Increased Costs of Working

We will cover You for any additional expenditure necessarily and reasonably incurred during the Indemnity Period as a direct result of a Cyber Incident or System Failure first discovered during the Period of Insurance and which directly affects Your Computer Equipment or the Computer Equipment of an Outsourced Service Provider, where such additional expenditure:

(a) has been incurred for the purpose of avoiding, reducing or preventing Loss of Profit arising from the Cyber Incident or System Failure, and

(b) shall be recoverable notwithstanding that such expenditure exceeds the amount of Loss of Profit avoided or reduced and regardless of the amount recoverable as Increased Costs of Working under this policy,

subject always to the applicable Cover Limit

Cover E: Consequential Reputational Harm

We will cover You for any Loss of Profits caused by the loss of a current or future customer sustained during the Indemnity Period as a direct result of a Cyber Incident or System Failure first discovered during the Period of Insurance, which directly affects Your Computer Equipment.

Section 4: Cyber Crime

Cover A: Funds Transfer Fraud

Where a Cyber Crime is first discovered during the Period of Insurance, We will cover You for

(1) the resulting financial loss

(2) costs and professional fees to substantiate the cause and the value of such loss, provided they are necessarily and reasonably incurred.

Cover B: Theft of Personal Money

We will cover You or Your partners, directors or Employees for the loss of personal money from Your or their personal bank account caused by a Third Party gaining unauthorised access to Your Computer Equipment, which is first discovered during the Period of Insurance.

Cover C: Telephone Hacking

We will cover the charges payable to Your supplier of Your telecommunications services which have been incurred as a result of unauthorised use of Your telecommunications services by a Third Party as a result of Hacking of Your Computer Equipment, which is first discovered during the Period of Insurance.

Cover D: Unauthorised Use of Computer Equipment

We will cover You for computing and power charges directly resulting from the unauthorised use of Your Computer Equipment by a Third Party, first discovered during the Period of Insurance, to:

(1) perform cryptocurrency mining

(2) carry out Hacking or a Denial of Service Attack

Section 5: Online Risk and Reputation

Cover A: Corporate Identity Fraud

Where Corporate Identity Fraud is first discovered during the Period of Insurance, We will cover You for reasonable and necessary

(1) fees, costs and expenses incurred by You in correcting or reinstating any public records following Corporate Identity Fraud. The public records must be held by an official registry or other similar party and relate to Your formation or identity and must be relied upon by investors or vendors to establish Your financial standing or credit worthiness

(2) legal fees, costs and expenses incurred by You in applying for any legal proceedings against You to be dismissed on the grounds that liability rests with a perpetrator of Corporate Identity Fraud against You, and

(3) fees, costs and expenses incurred by You in employing the services of a private investigation agency to identify the perpetrator of any Corporate Identity Fraud against You.

Cover B: Online Risk Response

Where an Online Risk Event, which directly affects You, has been first discovered during the Period of Insurance, We will cover You for the resulting reasonable and necessary cost of:

(1) accessing Our reputation protection services via Our 24/7 hotline

(2) obtaining initial advice and consultancy from Our reputation protection services provider

(3) engaging Our reputation protection services provider to coordinate and oversee the full response to the Online Risk Event, including platform monitoring, counselling for Employees, social media advice and crisis management

(4) legal fees to pursue takedown requests and injunctive relief

Cover C: Targeted Deepfake Attack

Where a Third Party has created and distributed Deepfake content purporting to be You or an Employee, which is first discovered during the Period of Insurance, We will cover You for the resulting reasonable and necessary cost of:

(1) accessing Our reputation protection services via Our 24/7 hotline

(2) obtaining initial advice and consultancy from Our reputation protection services provider

(3) engaging Our reputation protection services provider to coordinate and oversee the full response to the targeted Deepfake attack, including platform monitoring, counselling for Employees, social media advice and crisis management

(4) legal fees to pursue takedown requests and injunctive relief

Section 6: Network Security & Privacy Liability

Cover A: Network Security Liability

We will provide cover to You for Your legal liability to pay Compensation and Costs and Expenses in respect of any claim which is both first made against You during the Period of Insurance and notified to Us during the Period of Insurance or within 60 days of the expiry of the Period of Insurance and which arises from a Cyber Incident, and which results in:

(1) transmission of a Virus or Similar Mechanism

(2) unauthorised access to or use of Computer Equipment that results in Denial of Service Attack

(3) unauthorised access to Data stored on Your Computer Equipment or the Computer Equipment of an Outsourced Service Provider

Cover B: Privacy and Confidentiality Liability

We will provide cover to You for Your legal liability to pay Compensation and Costs and Expenses in respect of any claim which is both first made against You during the Period of Insurance and notified to Us during the Period of Insurance or within 60 days of the expiry of the Period of Insurance and which arises from an actual or alleged:

(1) disclosure of or unauthorised access to any Personal Data, including payment card data and protected health information

(2) failure to adequately warn Data Subjects of a Data Security Breach

(3) breach of any duty of confidence, including a breach of a non-disclosure agreement or a contractual warranty regarding the confidentiality of commercial information or Personal Data

(4) breach of Your privacy policy

(5) disclosure of or unauthorised access to Your Data or Third Party Data for which You are responsible

Cover C: Payment Card Industry Liability

Where, during the Period of Insurance, there has been an actual or suspected breach of payment card data as a direct result of a Cyber Incident, We will cover You for the reasonably and necessarily incurred costs of

(1) a payment card industry forensic investigator

(2) regaining certification

(3) any associated non-compliance fees or charges

(4) reissuance of cards

Cover D: Regulatory Fines and Penalties

We will cover You in respect of

(1) any lawfully insurable regulatory fines and penalties imposed on You by a governmental, regulatory, law enforcement, professional or statutory body

(2) legal costs necessarily and reasonably incurred by You to respond to or defend action taken by a governmental, regulatory, law enforcement, professional or statutory body

as a result of a breach of Data Protection Regulations arising as a direct result of a Cyber Incident.

Section 7: Multimedia Liability

Cover A: Defamation

We will provide cover to You for Your legal liability to pay Compensation and Costs and Expenses in respect of any claim which is both first made against You during the Period of Insurance and notified to Us during the Period of Insurance or within 30 days of the expiry of the Period of Insurance and which arises as a direct result of defamation of character, libel or slander which results from the use by You of Media in connection with The Business.

Cover B: Intellectual Property Infringement

We will provide cover to You for Your legal liability to pay Compensation and Costs and Expenses in respect of any claim which is both first made against You during the Period of Insurance and notified to Us during the Period of Insurance or within 30 days of the expiry of the Period of Insurance and which arises as a direct result of plagiarism or infringement of any trade mark, registered design or copyright committed or occasioned by You which results from the use by You of Media in connection with The Business.

Cover C: Media Removal Costs

We will pay costs, incurred with Our consent, for the removal of Your On-line Media content which will avoid a claim being made, or mitigate a claim that has been made, against You under this Section.

Exceptions

The following Exceptions apply to Section 7: Multimedia Liability in addition to the Policy Exceptions.

We will not provide cover for

Patent infringement

(1) any infringement of patents or misappropriation of trade secrets

Loss of economic value

(2) any future cost of doing business including but not limited to the value of any licence or royalty fee going forward

Professional Liability

(3) any liability arising from the provision of, or failure to provide, professional services or professional advice or a breach of any contract for the provision of professional services or professional advice.

Clauses

The following clauses are applicable to all Cyber Covers

Acquisition, Establishment or Disposal of Another Company

We will automatically extend the cover available under this policy where You establish or acquire a new subsidiary company during the Period of Insurance, provided that the newly established or acquired subsidiary company

(1) is not registered, and does not have any employees, operations or assets, outside of Great Britain, Northern Ireland, the Channel Islands or the Isle of Man, and

(2) has a gross annual turnover which is less than 10% of Your combined total gross turnover (including, for the avoidance of any doubt, those of any subsidiary company declared to Us immediately before the new acquisition or establishment), and

(3) has not had any incidents in the past three years which would or could have led to a claim under any of these cyber covers, and

(4) carries out business activities which are not materially different to The Business.

Unless automatic coverage applies, as set out above, You must

(1) give Us written notice of any such new acquisition or establishment as soon as practicable, together with such additional information as We may require, and

(2) accept any notified alteration to the terms of this policy, and

(3) pay any additional premium required by Us.

In the event that You do not accept any notified alteration to the terms of this policy or additional premium, You will have the right to decline coverage under this policy for the new subsidiary company.

Unless otherwise agreed, We will only cover the new subsidiary company under this policy from the date such new subsidiary company was established or acquired by You.

In the event of the liquidation or sale of a subsidiary company during the Period of Insurance, We will continue to cover such subsidiary company under this policy during this process but only in respect of claims which are notified to Us while the subsidiary company is part of Your group.

Mitigation of Loss

We will cover You for reasonable costs and expenses incurred by You in respect of any reasonable action taken to mitigate a loss or potential loss or Claim that would otherwise be the subject of indemnity under this policy provided that

(1) We give prior written consent to You incurring such costs and expenses

(2) You prove to Our satisfaction that the amount of the costs and expenses to be incurred are less than any likely award of damages arising from the same potential Claim or (as applicable) any potential loss.

Payment for Court Attendance

We will compensate You if, at Our request, You or any director, partner or Employee of Yours attend

court as a witness in connection with a claim for which You are entitled to cover. The maximum We will pay, per day, for You or each director, partner or Employee of Yours is stated in The Schedule.

The following clause is applicable to Section 3: Business Interruption

Payments on Account

Payments on account will be made if requested where We have admitted liability.

Exceptions

The following exceptions apply to all covers unless otherwise stated.

We will not provide cover for

Known Circumstances

(1) circumstances which, as of the Continuity Date of this policy, You knew or ought to have known about and which may give rise to a claim

Terrorism

(2) any Damage, or the threat thereof, or any consequence resulting directly or indirectly from or in connection with Terrorism regardless of any other cause or event contributing concurrently or in any other sequence to the loss. However We will provide cover for Cyber Terrorism.

Property Damage

(3) loss, destruction of or damage to property, other than as expressly covered in Section 2, Cover B: Hardware Replacement Costs or Section 4: Cyber Crime

Bodily Injury

(4) any death or Bodily Injury or disease suffered or alleged to be suffered by anyone.

However, this exception does not apply to any part of a covered Claim seeking Compensation for mental anguish or distress under Section 6, Cover B: Privacy & Confidentiality or Section 7, Multimedia Liability.

Natural Perils

(5) any loss or liability resulting from a physical cause or natural peril including, but not limited to, fire, flood, storm, lightning, frost, explosion, extremes of weather or temperature, escape of water, or solar wind/storm.

Fines and Penalties

(6) any fine, regulatory or statutory payment and/or any liquidated damages, or any amount payable under any penalty clause other than

(a) any lawfully insurable regulatory fines and penalties as covered under Section 6, Cover D: Regulatory Fines and Penalties

(b) non-compliance fees as covered under Section 6, Cover C: Payment Card Industry Liability

Consequential Loss

(7) consequential loss or Damage except as covered under Section 3, Business Interruption

Chargebacks

(8) any credit card company or bank, wholly or partially, reversing or preventing a payment transaction, except as covered under Section 6, Cover C: Payment Card Industry Liability

Nuclear

(9) any loss or liability arising directly or indirectly from or contributed to by:

(a) ionising radiations or contamination by radioactivity from any nuclear fuel or from any nuclear waste from the combustion of nuclear fuel; or

(b) the radioactive, toxic, explosive or other hazardous properties of any explosive nuclear assembly or nuclear component.

Fraud and Insolvency

(10) any fraud or dishonesty as determined by final adjudication, insolvency, financial default, conversion, conspiracy, inducement of breach of contract, malicious or illegal act, deceit, intimidation, personal spite, ill will or liability arising out of any intentional or deliberate act or omission by You other than an Employee who is not a director acting intentionally and outside of their scope of authority

Criminal Prosecutions

(11) any Costs and Expenses of criminal prosecution awarded against You

Unlawful Surveillance

(12) any loss or liability in respect of any actual or alleged unauthorised monitoring, tracking or profiling of any individual or Computer System, including but not limited to web-tracking, session recording, digital fingerprinting, behavioural monitoring, eavesdropping, wiretapping, or unauthorised audio or video recording committed by You or by a third party on Your behalf with Your knowledge and consent.

Unsolicited Communications

(13) loss or liability arising directly or indirectly from any actual or alleged violation of:

(a) the CAN-SPAM Act of 2003 or any subsequent amendments to that Act

(b) the Telephone Consumer Protection Act (TCPA) of 1991 or any subsequent amendments to that Act; or

(c) any other law, regulation or statute relating to unsolicited communication, distribution, sending or transmitting of any communication via telephone or any other electronic or telecommunications device.

Claims by Related Entities

(14) any proceedings or claims brought by a subsidiary, parent or associate company

Infrastructure Failure

(15) any loss or liability arising directly or indirectly out of any failure, interruption, disturbance, degradation, corruption, impairment or outage of services provided by any satellite provider, utility provider, internet service provider, telecommunications provider, domain name service, certificate authority or content delivery network. However, We will cover Your direct losses if such services are under Your direct operational control.

War

(16) any consequence whatsoever which is the direct or indirect result of any of the following, or anything connected with any of the following, whether or not such consequence has been contributed to by any other cause or event

(a) armed conflict involving physical force:

(i) by a state against another state, or

(ii) as part of a civil war, rebellion, revolution, insurrection, military action or usurpation of power, whether war be declared or not.

(b) nationalisation, confiscation, requisition, seizure, damage or destruction by or by order of any government or any local or public authority, and

(c) any action taken in controlling, preventing, suppressing or in any way relating to (16) (a) and/or (16)(b) above

Cyber Warfare

(17) any loss or liability arising directly or indirectly out of:

(a) a Cyber Operation used in conjunction with a War, or

(b) a Cyber Operation that has a major detrimental impact on

(i) the functioning of a Relevant State due to disruption to the availability, integrity or delivery of an Essential Service in that state; or

(ii) the security or defence of a Relevant state

We shall be entitled to refer to reasonable available evidence in support of Our position in respect of attribution. This shall include but not be limited to any Designated Official of a Relevant State attributing a Cyber Operation to another sovereign state, or asserting that a Cyber Operation has been carried out on behalf of or in support of another sovereign state

Excess

(18) The Excess

However the Excess will not apply to Section 1, Cover A: Crisis Management

Betterment

(19) any Costs or Expenses which result in You being in a better financial position or You benefitting from upgraded versions of Your Computer Equipment.

However this exception will not apply to costs incurred under Section 1, Cover H, Resilience Improvement Costs or Section 2, Cover B, Hardware Replacement (Bricking) Costs where existing versions of Your Computer Equipment are unavailable.

Contractual liability

(20) any liability assumed by agreement which would not have arisen in the absence of such agreement other than as expressly covered under Section 6, Cover C: Payment Card Industry Liability

Breach of competition law

(21) any actual or alleged breach of competition law, restraint of trade or unfair competition

Chemical Release

(22) We will not provide cover in respect of any losses arising from chemical, biochemical or biological release, discharge, dispersal or escape.

How Much We Will Pay

Limit of Indemnity

Where the basis of settlement is stated in The Schedule as 'Aggregate', then the maximum We will pay under this policy in any Period of Insurance shall not exceed the Total Cover Limit shown on The Schedule.

The maximum We will pay under any cover for any one claim in any Period of Insurance shall not exceed the applicable Cover Limit for that cover as shown in The Schedule, subject always to the Total Cover Limit. Where more than one Cover Limit is applicable in respect of a claim, then only the highest Cover Limit shall apply, subject always to the Total Cover Limit.

Where the basis of settlement is stated in The Schedule as 'Any One Claim', then the maximum We will pay under any cover for any one claim in any Period of Insurance shall not exceed the applicable Cover Limit for that cover as shown in The Schedule. Where more than one Cover Limit is applicable in respect of a claim, then only the highest Cover Limit shall apply.

Any claim subsequently arising from any circumstance notified to Us shall be deemed to have been made during the Period of Insurance in which the notice of such circumstances was first received by Us.

Related Incidents

Where more than one claim arises from the same Cyber Incident, System Failure, Cyber Crime or other originating cause, all of those claims will be treated as one claim, and only one Total Cover Limit, Cover Limit(s) and Excess shall apply.

Claims Conditions

The following conditions apply to all covers in addition to the policy conditions at the back of the policy.

Admission of Liability

In the event of a claim or the discovery of a circumstance that might give rise to a claim, You must not admit liability for or settle or attempt to settle any claim, or incur any related costs or expenses, without Our prior written consent.

Claims Notification

You shall notify Us as soon as practicable, but no more than 60 days after the end of the Policy or at the end of any applicable extended reporting period (as detailed below), and irrespective of the effect of any applicable Excess if You

(1) discover a Cyber Incident, Cyber Extortion, System Failure or Cyber Crime,

(2) receive any claim or notice of intention to make a claim,

(3) become aware of any circumstance that might give rise to a claim. Any claim subsequently arising from any circumstance notified to Us shall be deemed to have first been made during the Period of Insurance in which the notice of such circumstance was first received by Us.

Contact Information

Upon discovering any indicators of compromise within Your digital estate, You should in the first instance contact Aviva Cyber Claims via the 24/7 Cyber Incident Hotline:

- **Telephone**: 0800 051 4473
- **Email**: **cyberclaims@aviva.com**

Notification provided to the appointed Cyber Incident Crisis Manager shall be deemed to be valid notice to Us.

Consent to Incur Costs

You will seek Our consent prior to incurring any costs under this policy. However, You may proceed to incur costs without Our consent where they are incurred via Our Cyber Incident Crisis Manager or from a pre-approved vendor panel provided by Us.

Control of Defence and Co-Operation

In the event of a claim or loss or the discovery of a circumstance that might give rise to a claim or loss, We will be entitled, at Our own expense at any time, to take over and conduct in Your name (but at Our sole discretion) the defence or settlement of any such claim or loss provided always that, if there is any dispute between You and Us as to whether a claim should be defended, We cannot require You to continue to defend a claim unless a King's Counsel (whose identity is agreed with Us) advises that the claim should be defended.

If We do take over and conduct the defence or settlement of any such claim or loss You shall give Us (and any consultants, agents or advisers who may be appointed by Us) all such information and assistance as We may reasonably require and that is in Your power to provide.

Your duty to assist Us includes

(1) providing all such information, documents (including access to those held in computerised or electronic format), assistance, signed statements or depositions as may be required to facilitate compliance with any civil procedure rules, practice directions and pre-action protocols as may be issued

(2) ensuring that all documents and records that might be relevant or otherwise required by Us are preserved (and, in the case of documents or records that are computerised or otherwise held electronically, ensuring that they are retained in a readily retrievable form)

(3) taking all reasonable steps to effectively mitigate any claim or loss

(4) allowing Us to present the best possible defence of a claim within the time constraints available

(5) ensuring ready access to all and any information that We may require in the defence of a claim or investigation of a loss

(6) ensuring the payment of the Excess in conjunction with the terms of any settlement agreed by Us.

(7) not disclosing the existence of the Cyber Extortion Cover except for any disclosure required under applicable law to the relevant law enforcement authorities

Discharge of Liability

We may at any time pay the Cover Limit or the Total Cover Limit. We will not make any further payment except for costs and expenses incurred prior to the payment of the claim.

Extended Reporting Period

We will automatically grant, at no additional premium, an extended reporting period of 60 days following the expiry of the Period of Insurance. Subject to all other terms, conditions and exceptions of this policy, this extended reporting period will cover:

(1) in respect of Section 1: Cyber Incident Response Costs, Section 2: Computer and Data Rectification Costs and Section 3: Business Interruption, any Cyber Incident, Cyber Extortion or System Failure first discovered by You during the Period of Insurance and reported to Us during this extended reporting period;

(2) in respect of Section 6: Network Security and Privacy Liability, any claim first made against You during the Period of Insurance and reported to Us during this extended reporting period; and

(3) any circumstance that a director or partner became aware of during the Period of Insurance and which is reported to Us during this extended reporting period.

No cover will be given under this extended reporting period for any claim in respect of which You are entitled to cover under any other insurance, or would be entitled to cover under such insurance if its limit of liability were not exhausted.

Recoveries

Following a payment under this policy, any recoveries will be made in the following order:

(1) any costs and expenses incurred in relation to the recovery

(2) any losses suffered by You in excess of the Cover Limit or Total Cover Limit

(3) amounts paid by Us

(4) the Excess

Subrogation

Anyone making a claim under this policy must, at Our request and expense, do everything We reasonably require to enforce a right or remedy or obtain relief or indemnity from other parties to which We will become entitled or subrogated because of payment for or making good loss, destruction, damage, accident or injury.

We may require You to carry out such actions before or after We make any admission of or payment of a claim.

Policy Conditions

The following policy conditions apply to all covers unless otherwise stated and in addition to the cover conditions contained in The Schedule.

Alteration of Risk

If there has been any alteration to The Business after the effective date of this insurance which increases the risk of loss, or Your interest ceases except by will or operation of law, We will at Our option avoid the policy from the date of such alteration or when Your interest ceases, unless We accept the alteration.

Arbitration

If We accept liability but You disagree with the amount We offer to pay, the claim will be referred to an arbitrator who will be jointly appointed in accordance with statutory provisions.

Cancellation

(1) You may cancel this policy at any time after the date We have received the premium by providing at least 30 days' written notice to Us.

(2) If there is a default under Your Aviva credit agreement which finances this policy, We may cancel this policy by providing written notice to You in accordance with the default termination provisions set out in your Aviva credit agreement.

If Your policy is cancelled under (1) or (2) above, We will refund to You a proportionate part of the premium paid for the unexpired period. This is provided that, during the current Period of Insurance, there has been no:

(a) claim made under the policy for which We have made a payment

(b) claim made under the policy which is still under consideration

(c) incident which You are aware of and which is likely to give rise to a claim, and which has already been, or is yet to be, reported to Us

(3) Where there is no Aviva credit agreement to finance this policy, We will cancel this policy from the inception date if the premium has not been paid and no return premium will be allowed. Such cancellation will be confirmed in writing by Us to Your last known address.

Contracts (Rights of Third Parties)

A person who is not a party to this policy has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any terms of this policy. This does not affect any right or remedy of a third party which exists or is available apart from that Act.

Contribution

If the insurance provided by any of the above covers is also covered by another policy (or would be but for the existence of such above cover), We will only provide cover to You for any excess beyond the amount which would be payable under such other insurance had such above cover not been effected.

Fraud

If a claim made by You or anyone acting on Your behalf and with Your directors' or officers' knowledge is fraudulent or fraudulently exaggerated or supported by a false statement or fraudulent means or fraudulent evidence is provided to support the claim, We may:

(1) refuse to pay the claim,

(2) recover from You any sums paid by Us to You in respect of the claim,

(3) by notice to You cancel the policy with effect from the date of the fraudulent act without any return of premium.

If We cancel the policy under (3) above, then We may refuse to provide cover after the time of the fraudulent act. This will not affect any liability We may have in respect of the provision of cover before the time of the fraudulent act.

If this policy provides cover to any person other than You and a claim made by such person or anyone acting on their behalf is fraudulent or fraudulently exaggerated or supported by a false statement or fraudulent means or fraudulent evidence is provided to support the claim, We may:

(1) refuse to pay the claim,

(2) recover any sums paid by Us to You in respect of the claim (from You or such person depending on who received the sums or who benefited from the cover provided),

(3) by notice to You and such person cancel the policy provided for such person with effect from the date of the fraudulent act without any return of premium in respect of such cover.

If We cancel a person's cover under (3) above, then We may refuse to provide cover after the time of the fraudulent act. This will not affect any liability We may have under such cover occurring before the time of the fraudulent act.

Non Disclosure, Misrepresentation or Misdescription

(1) Before this policy was entered into

If You have breached Your duty to make a fair presentation of the risk to Us before the policy was entered into, then:

- where the breach was deliberate or reckless, We may avoid this policy and refuse all claims, and keep all premiums paid;
- where the breach was neither deliberate nor reckless, and but for the breach:
  - We would not have agreed to provide cover under this policy on any terms, We may avoid this policy and refuse all claims, but will return any premiums paid
  - We would have agreed to provide cover under this policy but on different terms (other than premium terms), We may require that this policy includes such different terms with effect from its commencement,

    and/or
  - We would have agreed to provide cover under this policy but would have charged a higher premium, Our liability for any loss amount payable shall be limited to the proportion that the premium We charged bears to the higher premium We would have charged, as outlined in Schedule 1 to the Insurance Act 2015.

(2) Before a variation was agreed

If You have breached Your duty to make a fair presentation of the risk to Us before any variation to this policy was agreed, then:

- where the breach was deliberate or reckless, We may cancel this policy with effect from the date of the variation, and keep all premiums paid;
- where the breach was neither deliberate nor reckless, and but for the breach:
  - We would not have agreed to the variation on any terms, We may treat this policy as though the variation was never made, but will return any additional premiums paid
  - We would have agreed to the variation but on different terms (other than premium terms), We may require that the variation includes such different terms with effect from the date it was made,

    and/or
  - We would have agreed to the variation but would have increased the premium, or would have increased it by more than We did, or would not have reduced it or would have reduced it by less than We did, Our liability for any loss amount payable shall be limited on a proportionate basis, as outlined in Schedule 1 to the Insurance Act 2015.

Sanctions

We shall not provide cover nor be liable to pay any claim or provide any benefit under this policy if to do so would expose Us to any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions laws or regulations of the European Union, United Kingdom or United States of America or any of its states.

Severability of Interest

If The Policyholder comprises more than one party, each operating as a separate and distinct entity, this policy shall apply in the same manner and to the same extent to each party as if they were separately and individually insured.

Provided that for the purposes of the Total Cover Limit; or any other cover limit stated in The Schedule or elsewhere in this policy (as the case may be), all of the parties insured under this policy shall be treated as one party so that there shall be only a single contract of insurance between

(a) Aviva as one party

and

(b) The Policyholder, as the other party.

Definitions

The following definitions apply to all covers and shall keep the same meaning wherever they appear unless an alternative definition is stated to apply. A defined word or phrase will start with a capital letter each time it appears in the policy.

Bad Actor

Any person who has perpetrated or colluded in an act that has directly resulted in a claim under any of the Cyber Covers.

Bodily Injury

Bodily injury including death, illness, disease or nervous shock but not including emotional distress or mental anguish.

Compensation

Any damages, including interest.

Computer Equipment

all computers and input, output, processing, intranets and communication facilities, including sensors and actuators, hardware, off-line media libraries, Data and related communication or open systems networks, extranets, any websites, telephone systems, any industrial control systems, any information technology to steer or control technical processes, any embedded systems or any other industrial information technology (including operational technology)

Continuity Date

The inception date of this policy or, if You have maintained uninterrupted insurance of the same type with Us, the date such insurance was first incepted with Us

Corporate Identity Fraud

Fraudulent modification, alteration or theft of Your identity by a Third Party.

Costs and Expenses

(1) Costs and expenses incurred with Our written consent

(2) Any claimant's legal costs for which You are legally liable

in connection with any event which is or may be the subject of a claim under this policy.

Cover Limit

The maximum amount We will pay under each cover, as stated in The Schedule.

Cyber Crime

Any act of theft, fraud or dishonesty committed by a Third Party that causes You loss as a result of

(1) an electronic instruction sent to a financial institution at which You hold an account, instructing it to move a fixed amount out of Your account, without Your Knowledge or consent.

(2) a phishing, vishing or other Social Engineering attack against any Employee that results in the transfer to a Third Party of

  (a) Your money, securities or property or,

  (b) money You are responsible for on behalf of a customer or supplier

(3) the theft of money or securities by electronic means from a financial institution at which You hold an account

Cyber Extortion

A demand for payment as a pre-condition to resolving Cyber Incident which, at the time the demand is made:

(1) prevents access to Data, or

(2) involves a credible threat made against You to

  (a) destroy, use or reveal to third parties Personal Data or sensitive business Data

  (b) cause Damage to Your Computer Equipment, or

  (c) prevent access to Your Computer Equipment

Cyber Extortionist

Any party committing or being an accessory to a Cyber Extortion.

Cyber Extortion Payment

A payment made by You to a Cyber Extortionist following a Cyber Extortion.

Cyber Incident

Any actual or suspected:

(1) Data Security Breach

(2) Denial of Service Attack

(3) Hacking

(4) Virus or Similar Mechanism

Cyber Incident includes incidents created or facilitated using artificial intelligence tools

Cyber Incident Crisis Manager

The company appointed by Us to handle Your claim notification.

Cyber Operation

The use of any Computer Equipment by, on behalf of, or in support of a sovereign state to disrupt, deny, degrade, exfiltrate, manipulate or destroy any data or Computer Equipment in or of another sovereign state.

Cyber Terrorism

Any act or series of acts or threat thereof of any person or group of persons, whether acting alone or on behalf of or in connection with any organisation through the use of computer systems, to destruct, disrupt or subvert any computer system, computer network, infrastructure, the Internet, the intranet, telecommunications and/or its content, with the intention to cause harm or committed for religious, ideological or political purposes (including, but not limited to, the influencing of any government and/or to put the public in fear).

Damage

Loss, destruction or damage.

Data

All information which is electronically stored or represented, or contained on any current and back-up disks, tapes or other materials or devices used for the storage of data including but not limited to operating systems, records, programs, software or firmware, code of series of instructions.

Data Protection Regulations

The Data Protection Act 2018 or the General Data Protection Regulation (Regulation (EU) 2016/679) or any Legislation implementing the General Data Protection Regulation, or any previous or any replacement legislation in respect of any of the foregoing or any other similar foreign or domestic regulation, law or statute

Data Security Breach

Loss, theft, disclosure, destruction or accidental release of

(1) Personal Data involving one or more Data Subjects which creates a risk of financial harm to the Data Subject or which triggers an obligation under any law or regulation to notify the Data Subject of such loss, theft, disclosure, destruction or accidental release

(2) other Data.

Data Storage Materials

Any materials or devices used for the storage or representation of Data including but not limited to disks, tapes, CD-ROMs, DVDs, memory sticks, memory cards or other materials or devices which may or may not also constitute Computer Equipment.

Data Subject

An individual who is the subject of Personal Data.

Deepfake

An image, video or audio that has been digitally altered or created using Computer Equipment.

Denial of Service Attack

Any actions or instructions with the ability to damage, interfere with, or otherwise affect the availability of Computer Equipment or Data, including but not limited to the generation of excess traffic into network addresses, the exploitation of system or network weaknesses, and the generation of excess or non genuine traffic within, between or amongst networks.

Designated Official

Any person holding one of the following positions, or equivalent, within a sovereign state

(a) Head of government

(b) Interior minister

(c) Foreign minister

(d) Defence minister

(e) Official representative of a national intelligence or security service.

Employee

Any person who is

(1) under a contract of service or apprenticeship with You, borrowed by or hired to You, a labour master or supplied by a labour master, employed by labour only sub-contractors, self-employed, under a work experience or training scheme, a voluntary helper while working under Your control in connection with The Business

(2) outworker or homeworker when engaged in work on Your behalf.

Essential Service

A service which is essential for the maintenance of critical societal or economic activities of a sovereign state including but not limited to financial institutions and associated financial market infrastructure, transport network, health services or utility services.

Excess

The amount specified in Your policy or The Schedule which shall apply once per Period of Insurance, regardless of the number of claims made or occurrences reported to Us during that period. You will repay any such amount paid by Us. This Excess applies to all covered claims under this policy, and no additional Excess will be imposed for subsequent claims within the same Period of Insurance.

Hacking

Unauthorised access to or malicious use of any computer or other equipment, component, system or item which processes, stores or retrieves Data whether Your property or not.

Increased Costs of Working

The additional expenditure including, but not limited to, overtime or additional labour costs required to keep or restore The Business trading and provided such costs are necessarily and reasonably incurred for the sole purpose of avoiding or diminishing a Loss of Profit during the Indemnity Period which but for that expenditure would have taken place and provided that such expenditure shall be limited to the amount of Loss of Profit avoided as a result.

Indemnity Period

The period beginning when the Loss of Profit or Increased Costs of Working are first sustained by The Business as a result of a covered Cyber Incident or System Failure provided that such losses and costs are first sustained during the Waiting Period and ending when the adverse impact on The Business ceases, such period being subject to the Maximum Indemnity Period shown on The Schedule.

Loss of Profit

The amount by which the Standard Revenue exceeds the actual Revenue during the Indemnity Period, less any savings during the Indemnity Period in business charges or expenses, payable out of Revenue, which reduce or cease in consequence of the loss.

Maximum Indemnity Period

The number of months stated in The Schedule.

Media

Any text, images, videos or sound distributed via Your website, extranet or intranet, social media presence or externally distributed e-mail.

Online Risk Event

Impersonation, ad scams, fake reviews, misinformation and disinformation carried out by a Third Party via online content, including search engines, social media and review platforms

Outsourced Service Provider

Any provider of information technology, data hosting or data processing services to You under contract excluding the supply of gas, electricity, water, satellite, telecommunication or internet service.

Period of Insurance

From the effective date until the expiry date, both shown in The Schedule, or any subsequent period for which We accept payment for renewal of this policy.

Personal Data

Data which relates to a natural person who can be identified from that data which is in Your possession.

Relevant State

Any sovereign state

(1) in which the Data or Computer Equipment affected by a Cyber Operation is physically located or stored

Revenue

The money paid or payable to You for services rendered or goods sold in the course of The Business.

Standard Revenue

The Revenue during that period in the 12 months immediately before the date of the Damage which corresponds with the Indemnity Period.

Standard Revenue may be adjusted to reflect any trends or circumstances which

(1) affect The Business before or after the Damage

(2) would have affected The Business had the Damage not occurred.

The adjusted figure will represent, as near as possible, the results which would have been achieved during the same period had the Damage not occurred.

Reward

Any reward or similar payment paid by You, with Our consent, for information leading to the conviction of a Bad Actor, or for the recovery in whole or in part of a direct financial loss.

Social Engineering

A Third Party directly or indirectly inducing or deceiving an Employee into delivering, paying or transferring money, securities or insured property by impersonating or falsely claiming to be another person or organisation including, but not limited to, Employees, directors, creditors, clients, law enforcement agencies or financial institutions

System Failure

Any, unintentional and unplanned malfunction, interruption or outage of Computer Equipment which is caused by a software bug, network failure, hardware failure, or human error in the operation or maintenance of the Computer Equipment.

Terrorism

Any act or acts caused or occasioned by any person(s) or group(s) of person(s) or so claimed for political, religious, ideological or similar purposes.

The Business

Activities directly connected with the business specified in The Schedule.

The Schedule

The document issued to You which specifies details of The Policyholder, Total Cover Limit, Cover Limits, Excess(es), Endorsements and Conditions applying to this policy

Third Party

Any person who is not

(1) an Employee, equity partner, director or member of Yours or of a subsidiary or a parent or related or group company of Yours

(2) working in collusion with an Employee, equity partner, director or member of Yours or of a subsidiary or a parent or related or group company of Yours

(3) an external auditor or accountant, insurance intermediary, financial adviser, factor, commission merchant, consignee or other similar agent or representative whose services are employed by You.

Total Cover Limit

The amount stated in The Schedule.

Virus or Similar Mechanism

Program code, programming instruction or any set of instructions with the ability to damage, interfere with, or otherwise adversely affect Computer Equipment or Data, whether involving self-replication or not, including, but not limited to trojan horses, worms and logic bombs.

Waiting Period

The period of time shown in The Schedule.

We/Us/Our/Aviva

Aviva Insurance Limited.

You/Your/The Policyholder

The person, persons, company, companies, partnership, partnerships, unincorporated association or unincorporated associations named in The Schedule as The Policyholder.