

DECLARATIONS CYBER INSURANCE POLICY

THIS INSURANCE POLICY PROVIDES COVERAGE ON A CLAIMS-MADE AND REPORTED BASIS AND APPLIES ONLY TO CLAIMS FIRST MADE AND REPORTED TO THE INSURER DURING THE POLICY PERIOD OR ANY APPLICABLE EXTENDED PERIOD.

DEFENSE EXPENSES, WHERE APPLICABLE, ARE INCLUDED IN THE LIMITS OF INSURANCE, AND PAYMENT THEREOF WILL ERODE, AND MAY EXHAUST THE LIMITS OF INSURANCE.

PLEASE READ YOUR POLICY CAREFULLY.

The words "You" and "Your" refer to the **Named Insured** shown in the Declarations. The words "We", "Us" and "Our" refer to the Company providing this insurance.

In return for the payment of premium, and subject to all the terms and conditions of this Policy, We agree with You to provide the insurance as stated in this Policy.

Policy Information

Company Name:	Spinnaker Insurance Company
Producer Name:	Cowbell Insurance Agency LLC 6800 Koll Center Pkwy, Suite 250 Pleasanton, CA 94566
Named Insured:	
Policy Number:	
Mailing Address:	
Policy Period: From: To: 12:01 AM standard time at the Insured's mailing address shown above	
Website Address(es) / Domain(s)	

Coverage Information

Annual Premium	
Fees / Assessments <i>Included in Annual Premium unless otherwise noted</i>	
Retroactive Dates:	
Supplemental Extended Reporting Period	

Policy Aggregate Limits, Aggregate Sublimits, and Deductibles

Policy Aggregate Limit of Insurance:	
Policy Deductible Amount:	\$ <i>Per Cyber Incident, Extortion Threat, Security Breach, Wrongful Act, Interrelated Wrongful Acts, or Claim</i>
Insuring Agreement 1. Security Breach Response Expense	
Insuring Agreement 1. Reputational Harm Aggregate Sublimit	
Insuring Agreement 2. Extortion Threat and Ransom Payments	
Insuring Agreement 3. Recovery or Restoration of Electronic Data	Included at Policy Limit
Insuring Agreement 4. Business Income and Extra Expense Aggregate Sublimit	
Business Income Time Deductible:	
Insuring Agreement 5. Court Attendance Costs Aggregate Sublimit	
Insuring Agreement 6. Security Breach Liability	
Insuring Agreement 6. Regulatory Proceedings	Included at Policy Limit
Insuring Agreement 6. Funds Transfer Liability Aggregate Sublimit	
Insuring Agreement 7. Reputational Harm Sublimit	Included in Business Income and Extra Expense Aggregate Sublimit
Reputational Harm Time Deductible:	
Optional Endorsement Sublimits and Deductibles	
Funds Transfer Fraud Coverage Limit:	
Funds Transfer Fraud Coverage Deductible:	
Social Engineering Coverage Limit:	
Social Engineering Coverage Deductible:	
Invoice Manipulation Coverage Limit:	
Invoice Manipulation Deductible:	
Breach Costs Outside of Limits Coverage Limit:	
Service Fraud and Cryptojacking Coverage Limit:	

Endorsements

Endorsement Name:	Effective Date	Coverage Limit
Nebraska Changes SP NE 04 12 25		
Nebraska Changes - Cancellation and Nonrenewal SP NE 02 07 23		
Trade or Economic Sanctions SP CW 96 05 22		
Policyholder Disclosure - Notice of Terrorism Insurance Coverage SP CW 67 02 23		
Electronic Delivery Policy SP CW 94 05 22		
Privacy Disclosure Spinnaker - Privacy Policy		
Signature Page SP CW 93 05 22		
Additional Insured SP CW 89 12 25		
Invoice Manipulation Endorsement SP CW 82 12 25		
Telecommunications Fraud Endorsement SP CW 85 05 22		
Hardware Replacement Costs Endorsement SP CW 86 12 25		
Website Media Content Liability SP CW 83 05 22		
Post Breach Remediation Coverage Endorsement SP CW 87 05 22		
Service Fraud Including Cryptojacking SP CW 70 02 23		
Dedicated Breach Costs SP CW 71 12 25		
Funds Transfer Fraud & Social Engineering Endorsement SP CW 49 12 25		
Contingent Business Income - System Failure (IT) SP CW 62 12 25		
Contingent Business Income - Security Failure SP CW 63 12 25		
Blanket Additional Insured Endorsement SP CW 58 12 25		

Claims Information

To report Claims, please use the contact information below:

Phone Number: 833-633-8666

Email: claims@cowbellcyber.ai

SPECIMEN

COMMERCIAL CYBER INSURANCE POLICY

THIS POLICY IS A CONTRACT OF INSURANCE BETWEEN YOU AND US. YOUR POLICY CONTAINS ALL THE DETAILS OF THE COVERAGE THAT WE PROVIDE. THIS POLICY CONSISTS OF AND MUST BE READ TOGETHER WITH THE DECLARATIONS PAGE AND ANY ENDORSEMENTS.

THE INSURANCE PROVIDED UNDER THIS POLICY FOR CLAIMS MADE AGAINST YOU IS ON A CLAIMS MADE AND REPORTED BASIS, AND APPLIES TO CLAIMS ONLY IF THEY ARE FIRST DISCOVERED BY YOU DURING THE POLICY PERIOD AND REPORTED TO US DURING THE POLICY PERIOD OR ANY APPLICABLE EXTENDED REPORTING PERIOD.

THE SECURITY BREACH LIABILITY INSURING AGREEMENT CONTAINED IN THIS POLICY PROVIDES COVERAGE FOR DEFENSE EXPENSES WHICH ARE PAYABLE WITHIN, AND NOT IN ADDITION TO, THE LIMIT OF INSURANCE. PAYMENT OF DEFENSE EXPENSES UNDER THIS POLICY WILL REDUCE THE LIMIT OF INSURANCE.

PLEASE READ THE ENTIRE POLICY CAREFULLY.

Various provisions in this Policy restrict coverage. Read the entire Policy carefully to determine rights, duties and what is and is not covered.

Throughout this Policy, the words "You" and "Your" refer to the **Named Insured** shown in the Declarations. The words "We," "Us," and "Our" refer to the company providing this insurance.

All terms that appear in bold print are defined terms and have special meaning as set forth in Section I – Insuring Agreements and Section VII – Definitions.

SECTION I – INSURING AGREEMENTS

Coverage is provided under the following Insuring Agreements up to the Limits of Insurance shown in the Declarations.

Any **Cyber Incident**, **Extortion Threat**, **Security Breach**, or **Claim** that arises out of the same facts or circumstances and results in **Loss** under one or more of the following Insuring Agreements will be deemed to be related and, as such, will be deemed to have been **Discovered** during the earliest **Policy Period** that any such related **Cyber Incident**, **Extortion Threat**, **Security Breach**, or **Claim** was **Discovered**.

1. Security Breach Response Expense

We will pay for **Loss** resulting directly from a **Security Breach** or **Cyber Incident** that is **Discovered** during the **Policy Period** or any **Extended Reporting Period**, if applicable.

With respect to this Insuring Agreement 1, **Loss** means:

a. Forensics Expenses – Including Breach Counsel Expenses

The costs incurred, with Our approval, to establish whether a **Security Breach** or **Cyber Incident** has occurred or is occurring.

If a **Security Breach** has occurred, the following costs are also included:

- i. costs to investigate the cause, scope and extent of a **Security Breach** and to identify any affected parties; and

- ii. costs to determine any action necessary to remediate the conditions that led to or resulted from a **Security Breach** including, but not limited to, fees paid for legal and other professional advice on how to respond to the **Security Breach**.

b. Notification Expenses – Including Breach Counsel Expenses

Costs to notify all parties affected by a **Security Breach** including, but not limited to, notice to be transmitted through media:

- i. as required by **Privacy Regulations**; or
- ii. subject to Our prior approval, as appropriate on a voluntary basis.

c. Overtime Salaries

Reasonable overtime salaries paid to **Employees** assigned to handle inquiries from the parties affected by a **Security Breach**.

d. Call Center Expenses

Fees and costs of a company hired by You with Our prior approval for the purpose of operating a call center to handle inquiries from the parties affected by a **Security Breach**.

e. Post-event Monitoring Expenses

Costs to provide credit and identity monitoring services to the affected parties of a **Security Breach** for up to one year, or longer if required by applicable law, from the date of notification to those affected parties of such **Security Breach**.

f. Public Relations Expenses

Fees and costs of a public relations firm and any other reasonable expenses incurred by You with Our prior written consent to protect or restore Your reputation solely in response to “negative publicity”.

As used in this provision, “negative publicity” means information which has been made public that has caused, or is reasonably likely to cause, a decline or deterioration in the reputation of the **Named Insured** or of one or more of its products or services.

g. Other Expenses

Any other reasonable expenses incurred by You in connection with a **Security Breach** or **Cyber Incident** with Our prior written consent.

With respect to this Insuring Agreement 1, **Loss** does not include any costs or expenses associated with upgrading or improving a **Computer System** as a result of a **Security Breach**.

2. Extortion Threats

We will pay for **Loss** resulting directly from an **Extortion Threat** that is **Discovered** during the **Policy Period** or any **Extended Reporting Period**, if applicable.

With respect to this Insuring Agreement 2, **Loss** means:

- a. Fees and costs of:
 - i. a cybersecurity firm or incident response provider; or

- ii. a person or organization;

hired with Our consent to determine the validity and severity of an **Extortion Threat** made against You.

- b. Interest costs paid by You for any loan from a financial institution taken by You to pay a ransom demand.
- c. Reward payments paid by You to an “informant” which leads to the arrest and conviction of any party responsible for **Loss**. Reward payments do not include any amount based on information provided by the **Insured**, the Insured’s auditors, or any individual hired or retained to investigate the illegal acts.

As used in this provision, “informant” means a person, other than an **Employee**, providing information not otherwise obtainable, solely in return for a reward offered by You.

- d. Any other reasonable expenses incurred by You with Our written consent, including, but not limited to:
 - i. fees and costs of independent negotiators; and
 - ii. fees and costs of a company hired by You, upon the recommendation of the security firm, to determine how to protect Your **Electronic Data** from further threats.
- e. Monetary value of any **Ransom Payment** made by You to a third party for **Ransom Demands**.

3. **Recovery or Restoration of Electronic Data**

We will pay for **Loss** of Your **Electronic Data** or “computer programs” stored within a **Computer System** resulting directly from a **Cyber Incident** that is **Discovered** during the **Policy Period** or any **Extended Reporting Period**, if applicable.

With respect to this Insuring Agreement 3, **Loss** means the costs to replace or restore Your **Electronic Data** or “computer programs” as well as the cost of data entry, reprogramming and computer consultation services.

With respect to this Insuring Agreement 3, **Loss** does not include the cost to duplicate research that led to the development of Your **Electronic Data** or “computer programs”. To the extent that any of Your **Electronic Data** cannot be replaced or restored, We will pay the cost to replace the media on which such **Electronic Data** was stored with blank media of substantially identical type.

As used in this Insuring Agreement 3, “computer programs” means a set of related electronic instructions, which direct the operation and function of a computer or devices connected to it, which enables the computer or devices to receive, process, store or send Your **Electronic Data**.

4. **Business Income and Extra Expense (Security Failure and System Failure)**

We will pay for **Loss** incurred during an **Interruption** resulting directly from a;

- a. **Cyber Incident**;
- b. **Extortion Threat**; or
- c. **System Failure** of Your **Computer System**;

that is **Discovered** during the **Policy Period** or during any **Extended Reporting Period**, if applicable.

With respect to this Insuring Agreement 4, **Loss** means the actual **Loss** of: (1) “business income” You sustain; and/or (2) “extra expense” You incur. **Loss** does not include: (1) **Loss** arising out of any liability to any third party; and/or (2) Legal costs or expenses.

As used in this Insuring Agreement 4:

a. “Business income” means the:

- i. net income (net profit or loss before income taxes) that would have been earned or incurred; and
- ii. continuing normal operating expenses incurred, including payroll.

“Business income” does not include:

- (1) Continuing normal operating expenses incurred, including payroll, if there has been no net income (net profit or loss before income taxes) that would have been earned or incurred as set forth in paragraph a.i. above; and/or
- (2) Net Profit that would likely have been earned as a result of an increase in volume due to favorable business conditions caused by the impact of network security failures impacting other businesses, loss of market, or any other consequential loss.

b. “Extra expense” means necessary and reasonable expenses You incur:

- i. during an **Interruption** that You would not have incurred if there had been no **Interruption**; or
- ii. during an **Interruption** to avoid or minimize the suspension of Your business operations.

“Extra expense” does not include:

- (1) any costs or expenses associated with upgrading, maintaining, repairing, remediating or improving a **Computer System** as a result of a **Cyber Incident, Extortion Threat, or System Failure**; or
- (2) **Extortion Expenses** covered under Insuring Agreement 2 – Extortion Threats.

5. Court Attendance Costs

We will pay for the reasonable and necessary costs and expenses of You attending, at our request, a trial, hearing, deposition, mediation, arbitration, or other proceeding relating to the defense of any **Claim**.

6. Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties

We will pay for:

- a. **Loss** that the **Insured** becomes legally obligated to pay and **Defense Expenses** as a result of a **Claim** that is **Discovered** during the **Policy Period** or any **Extended Reporting Period**, if applicable, for a **Wrongful Act** or a series of **Interrelated Wrongful Acts** taking place on or after Your first date of continuous coverage with Us and before the end of the **Policy Period**.
- b. **Loss** and **Defense Expenses** as a result of a **Claim** in the form of a **Regulatory Proceeding** that is **Discovered** during the **Policy Period** or any extended reporting period, if applicable, in response to a **Wrongful Act** or a series of **Interrelated Wrongful Acts** taking place on or after Your first date of continuous coverage with Us and before the end of the **Policy Period**.
- c. **Loss** and **Defense Expenses** as a result of a **Claim** in the form of an action by a **Card Company** for non-compliance with the Payment Card Industry (PCI) Data Security Standards

that is **Discovered** during the **Policy Period** or any extended reporting period, if applicable, in response to a **Wrongful Act** or a series of **Interrelated Wrongful Acts** taking place on or after Your first date of continuous coverage with Us and before the end of the **Policy Period**.

- d. **Loss** that the **Insured** becomes legally obligated to pay and **Defense Expenses** as a result of a **Claim** that is **Discovered** during the **Policy Period** or any **Extended Reporting Period**, if applicable, for a **Funds Transfer Liability Loss** taking place on or after Your first date of continuous coverage with Us and before the end of the **Policy Period**.

With respect to this Insuring Agreement 6:

i. **Loss** means:

- (1) compensatory damages, settlement amounts and costs awarded pursuant to judgments or settlements;
- (2) punitive and exemplary damages to the extent such damages are insurable by law;
- (3) fines or penalties assessed against the **Insured** to the extent such fines or penalties are insurable by law; or
- (4) the monetary amount owed by You under the terms of a PCI merchant services agreement with a **Card Company** as a direct result of a **Security Breach**.

Loss does not include:

- (a) civil or criminal fines or penalties imposed by law, except civil fines or penalties as provided under Paragraph i.(3) above;
- (b) the multiplied portion of multiplied damages;
- (c) taxes;
- (d) royalties;
- (e) the amount of any disgorged profits;
- (f) matters that are uninsurable pursuant to law;
- (g) any fees resulting from the recall, re-performance or correction of services, content, goods or activities;
- (h) the costs to comply with injunctive or other non-monetary relief; or
- (i) liquidated damages pursuant to a contract, to the extent such amount exceeds the amount for which You would have been liable in the absence of such contract, except for amounts under Paragraph i.(4) above.

- ii. **Defense Expenses** means the reasonable and necessary fees (attorneys' and experts' fees) and expenses incurred in the defense or appeal of a **Claim**, including the cost of appeal, attachment or similar bonds (without any obligation on Our part to obtain such bonds) but excluding wages, salaries, benefits or expenses of Your **Employees**.

iii. **Wrongful Act** means any actual or alleged:

- (1) **Security Breach**;
- (2) failure to prevent unauthorized access to, or use of, electronic or non-electronic data containing **Personal Information**;
- (3) failure to prevent the transmission of a **Virus** through a **Computer System** into a computer network, any application software, or a computer operating system or related network that is not rented, owned, leased by, licensed to or under the direct operational control of the **Insured**; or
- (4) failure to provide notification of any actual or potential **Security Breach** if such notification is required by any security breach notification law;

by, or asserted against, an **Insured**.

- iv. **Interrelated Wrongful Acts** means all **Wrongful Acts** that have as a common nexus any i) fact, circumstance, situation, event, transaction or cause; or ii) series of causally connected facts, circumstances, situations, events, transactions or causes.
- v. **Regulatory Proceeding** means an investigation, demand or proceeding brought by, or on behalf of, the Federal Trade Commission, Federal Communications Commission, the Department of Health and Human Services or other administrative or regulatory agency, or any federal, state, local or foreign governmental entity in such entity's regulatory or official capacity, including, but not limited to any investigation, demand, or proceeding, brought by an administrative or regulatory agency whether involving the California Consumer Privacy Act (CCPA), the General Data Protection Regulation (GDPR), or similar privacy regulations.
- vi. **Funds Transfer Liability** means the distribution of fraudulent wire transfer or payment instructions, which instruction purports to have been transmitted by You directing Your **Vendor** to transfer funds to a third party, but was transmitted by someone other than You as a result of a **Security Breach**.
- vii. **Funds Transfer Liability Loss** means a monetary judgment 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** by Your **Vendor**, to a third party as the direct result of a **Funds Transfer Liability**.
- viii. **Vendor** means:
 - (1) a natural person or entity who exchanges, or is under contract to exchange, goods or services with the **Named Insured** for a fee (other than a financial institution, asset manager, broker-dealer, armored motor vehicle "named insured" or any similar entity); or
 - (2) a computer software contractor who has a written agreement with the **Named Insured** to design, implement or service **Computer Programs** for a covered **Computer System**;provided such person, entity or contractor is not owned, operated, or controlled by the **Named Insured**.

7. **Reputational Harm**

We will pay for **Loss** resulting directly from an **Adverse Publication** specifically concerning a **Cyber Incident**, **Extortion Threat**, or **Security Breach** that is **Discovered** during the **Policy Period** or during any **Extended Reporting Period**, if applicable.

With respect to this Insuring Agreement 7, **Loss** means: the net income (net profit or loss before income taxes) incurred by the **Insured** during the **Reputational Harm Indemnity Period** that would have been earned or avoided had no **Adverse Publication** occurred.

Loss does not include:

- i. **Loss** arising out of any liability to any third party;
- ii. Costs to rehabilitate Your reputation;
- iii. Legal costs or expenses;
- iv. **Loss** arising out of Security Breach Response Expenses; and/or
- v. **Loss** arising out of an actual or alleged interruption of Your business operations for any period of time.

SECTION II – LIMITS OF INSURANCE

1. Policy Aggregate Limit of Insurance

The most We will pay for all covered **Loss** and **Defense Expenses** is the Policy Aggregate Limit of Insurance shown in the Declarations. The Policy Aggregate Limit of Insurance shall be reduced by any payment, including **Defense Expenses**, made under the terms of this Policy. Upon exhaustion of the Policy Aggregate Limit of Insurance by such payments, We will have no further obligations or liability of any kind under this Policy.

2. Aggregate Sublimit(s) of Insurance

Any Aggregate Sublimit(s) of Insurance set forth in the Declarations are part of, and not in addition to, the Policy Aggregate Limit of Insurance. Any such Aggregate Sublimit(s) of Insurance shall be reduced by any payment for **Loss** and, if applicable, **Defense Expenses**, under the Insuring Agreement to which such Aggregate Sublimit of Insurance applies. Upon exhaustion of any Aggregate Sublimit of Insurance by such payments, We will have no further obligations or liability of any kind with respect to **Loss** or **Defense Expenses**, subject to such Sublimit of Insurance.

SECTION III – DEDUCTIBLE

Subject to Section II – Limits of Insurance:

1. Under Insuring Agreements 1 – Security Breach Response Expense, 2 – Extortion Threats and 3 – Recovery or Restoration of Electronic Data, We will pay only the amount of **Loss** which is in excess of the Policy Deductible amount shown in the Declarations.

2. Under Insuring Agreement 4 – Business Income and Extra Expense (Security Failure and System Failure) and Insuring Agreement 7 – Reputational Harm:

We will pay only the amount of **Loss** which exceeds the greater of the following deductible amounts:

- a. The Policy Deductible Amount shown in the Declarations; or
- b. The amount of **Loss** incurred during the applicable Time Deductible shown in the Declarations.

3. Under Insuring Agreement 6 – Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties:

We will pay only the amount of **Loss** and **Defense Expenses**, which is in excess of the Policy Deductible Amount shown in the Declarations, resulting from the same **Wrongful Act** or **Interrelated Wrongful Acts**. Such Policy Deductible Amount will be borne by You, self-insured, and at Your own risk.

4. The Policy Deductible applies separately to each **Cyber Incident**, **Extortion Threat**, **Security Breach**, **Wrongful Act**, **Interrelated Wrongful Acts**, or **Claim**. In the event a **Loss** is covered under more than one Insuring Agreement, only the single highest deductible amount applicable to the **Loss** shall be applied.

SECTION IV – DEFENSE AND SETTLEMENT

The provisions contained within this section apply only to Insuring Agreement 6 – Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties:

We shall have the right and duty to select counsel and defend the **Insured** against any **Claim** covered under Paragraph 6.a of Insuring Agreement 6 – Security Breach Liability Including Payment Card Industry (PCI) Fines

and Penalties, even if the allegations of such **Claim** are groundless, false or fraudulent. However, We shall have the right but not the duty to defend the **Insured** against a **Claim** covered under Paragraphs 6.b or 6.c. of Insuring Agreement 6 - Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties. We shall have no duty to defend the **Insured** against any **Claim** which is not covered under an Insuring Agreement.

We may, upon the written consent of the **Insured**, make any settlement of a **Claim** which We deem reasonable. If the **Insured** withholds consent to such settlement, Our liability for all **Loss** resulting from such **Claim** will not exceed the amount for which We could have settled such **Claim**, plus **Defense Expenses** incurred, as of the date We proposed such settlement in writing to the Insured. Upon refusing to consent to a settlement We deem reasonable, the **Insured** shall, at its sole expense, assume all further responsibility for its defense, including all additional **Defense Expenses**, costs associated with the investigation, defense and/or settlement of such **Claim**.

SECTION V – EXCLUSIONS

We will not be liable for **Loss** or **Defense Expenses** directly or indirectly based upon, attributable to or arising out of:

1. Lightning, earthquake, hail, volcanic action, wind, smoke, explosion, tidal wave or flood, landslide, electromagnetic pulse, or other electromagnetic disturbances and/or any Space Weather as classified by NOAA, tornado, or any other act of God or nature.
2. Any of the following:
 - a. War, including undeclared or civil war or civil unrest;
 - b. Warlike action by military force, including action hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents;
 - c. Insurrection, rebellion, revolution, usurped power or action taken by government authority in hindering or defending against any of these;
 - d. Any **Cyber Incident**, **Security Breach**, or other **Wrongful Act** by or on behalf of any government, sovereign, state, or other authority sponsored actor or group that results in, or is carried out in the course of, any of the events in Paragraph a, b, or c above.
3. The dispersal or application of pathogenic or poisonous biological or chemical materials, nuclear reaction, nuclear radiation or radioactive contamination, or any related act or incident, however caused.
4. **Bodily Injury** or physical damage to or destruction of tangible property, including loss of use thereof.

Bodily Injury means bodily injury, sickness or disease sustained by a person, including death resulting from any of these at any time. It also means mental injury, mental anguish, mental tension, emotional distress, pain or suffering or shock sustained by any person.

However, **Bodily Injury** does not mean mental anguish or emotional distress resulting directly from a **Security Breach** or **Cyber Incident**.

5. Any disruption in normal computer function or network service or function due to insufficient capacity to process transactions or due to an overload of activity on a **Computer System** or network. However, this exclusion shall not apply if such disruption is caused by a **Cyber Incident** or **Security Breach**.
6. Any disruption of i) internet service; or ii) any external telecommunication network, regardless of the cause; or iii) failure or termination of any core element of internet, telecommunications, or GPS infrastructure that results in a regional, countrywide, or global outage of such infrastructure; or iv) failure of power supply and other utilities unless the provision of power and other utility services is under the **Named Insured's** direct control.

However, parts i) and ii) of this exclusion shall not apply if such disruption is caused by a denial of service attack under Paragraph b. of Definition 7. **Cyber Incident**.

7. Any failure of, reduction in or surge of power, regardless of the cause.
 8. Any actual or alleged violation of the Racketeer Influenced and Corrupt Organizations Act (RICO) and its amendments, or similar provisions of any federal, state or local statutory or common law.
 9. Any malfunction or failure of any satellite.
 10. Any actual or alleged oral or written publication of material, if done by an **Insured** or at an **Insured's** direction with knowledge of its falsity.
 11. An **Insured's** assumption of liability by contract or agreement, whether oral or written. However, this exclusion shall not apply to any liability that an **Insured** would have incurred in the absence of such contract or agreement.
 12. Any actual or alleged patent or trade secret violation, including any actual or alleged violation of the Patent Act, the Economic Espionage Act of 1996 or the Uniform Trade Secrets Act and their amendments.
 13. Any of the following:
 - a. The actual, alleged or threatened discharge, dispersal, seepage, migration, release or escape of **Pollutants** at any time;
 - b. Any request, demand, order or statutory or regulatory requirement that any **Insured** or others test for, monitor, clean up, remove, contain, treat, detoxify or neutralize, or in any way respond to, or assess the effects of, **Pollutants**; or
 - c. Any **Claim** or **Suit** brought by, or on behalf of, any governmental authority for damages because of testing for, monitoring, cleaning up, removing, containing, treating, detoxifying or neutralizing, or in any way responding to, or assessing the effects of, **Pollutants**.
 14. Any **Claim**, **Suit** or other proceeding against an **Insured** which was pending or existed prior to the Policy Period or arising out of the same or substantially the same acts, facts, circumstances or allegations which are the subject of, or the basis for, such **Claim**, **Suit** or other proceeding.
 15. Any actions or activities related to an **Insured's** practices as an employer including, but not limited to, refusal to employ, termination of employment, coercion, demotion, evaluation, reassignment, discipline, defamation, harassment, humiliation, discrimination or malicious prosecution. This exclusion applies:
 - a. Whether the injury-causing event described above occurs before employment, during employment or after employment of that person;
 - b. Whether the **Insured** may be liable as an employer or in any other capacity; and
 - c. To any obligation to share damages with or repay someone else who must pay damages because of the injury.
- However, this exclusion will not apply to any **Claim** resulting directly from a **Security Breach** related to the **Personal information** of an **Employee**.
16. Any **Cyber Incident**, **Extortion Threat**, **Security Breach**, **Wrongful Act**, or **Interrelated Wrongful Acts** that any **Insured** became aware of prior to the effective date of the Policy.
 17. The same facts, **Cyber Incident**, **Extortion Threat**, **Security Breach**, **Wrongful Act**, or **Interrelated Wrongful Acts** alleged or contained in any **Claim** which has been reported, or in any circumstances of which notice has been given, under any insurance policy of which this Policy is a renewal or replacement.

18. Any criminal, dishonest, malicious or fraudulent act, error or omission or any willful violation of any statute or regulation committed by an **Insured**, acting alone or in collusion with others.

However, with the exception of **Claims** excluded under Exclusion 12., this exclusion shall not apply to any dishonest, malicious or fraudulent act, error or omission committed by an **Employee** which gives rise to a **Claim** or **Loss** covered under Insuring Agreement 1 – Security Breach Response Expense or Insuring Agreement 6 – Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties. This exception does not apply to any **Employee** who is a Chief Executive Officer, Chief Financial Officer, Chief Security Officer, Chief Technology Officer, Chief Information Officer, Risk Manager, General Counsel, owner, general manager or any functionally equivalent positions of the **Insured** or any **Subsidiary**, regardless of title.

With the exception of **Claims** excluded under Exclusion 12, We will defend the **Insured** against any **Claim** alleging such acts or violations until final adjudication is rendered against that **Insured**. Final adjudication rendered against one **Insured** shall not be imputed to any other **Insured**.

We will not provide indemnification for any **Claim** to which any **Insured** enters a guilty plea or pleads no contest and We will not provide a defense from the time We become aware that any **Insured** intends to so plead.

19. Any action or proceeding brought by, or on behalf of, any governmental authority or regulatory agency including, but not limited to:
- a. The seizure or destruction of property by order of a governmental authority;
 - b. Regulatory actions or proceedings brought by, or on behalf of, the Federal Trade Commission, Federal Communications Commission or other regulatory agency, except when covered under Paragraph c. a of Insuring Agreement 6 – Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties; or
 - c. The shutdown or seizure of systems or services by a government or regulatory body.

However, this exclusion shall not apply to actions or proceedings brought by a governmental authority or a regulatory agency acting solely in its capacity as a customer of the **Named Insured** or of a **Subsidiary**.

20. Any costs or expenses associated with upgrading or improving a **Computer System** regardless of the reason.
21. Any **Claim** brought or alleged by one **Insured** against another, except for a **Claim** brought or alleged by an **Employee** against an **Insured** as a result of a **Security Breach** or **Cyber Incident**.
22. Fines, penalties or assessments imposed pursuant to contract or agreement, whether oral or written. This exclusion shall not apply to the coverage provided under Paragraph c. of Insuring Agreement 6 - Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties.
23. Any costs related to loss of any virtual currency.
24. Any actual or alleged restraint of trade, monopolization, unfair trade, price fixing, violation of the Federal Trade Commission Act, the Sherman Antitrust Act, the Clayton Act, including any amendment thereto or any rule or regulation promulgated under any such statute, or any similar foreign, federal, state or local statute, rule or regulation. However, this exclusion shall not apply to a **Claim** alleging unfair or deceptive acts or practices in or affecting commerce under Section 5(a) of the Federal Trade Commission Act (15 U.S.C. 45(a)).
25. Any of the following:
- a. Unlawful or unauthorized collection, harvesting, processing, storage, transfer, distribution or sale of **Personal Information** or other data;

- b. Wiretapping, eavesdropping, improper consent practices, unlawful or unauthorized use of tracking/monitoring/surveillance software tools, or audio or video recording; or
- c. Violation of the Illinois Biometric Information Privacy Act or similar provisions of any federal, state, local, or foreign statutory or common law, directive or regulation regulating the collection, handling, use, or storage of biometric data and/or any required disclosures thereof.

However, section 25.a of this exclusion will not apply to **Defense Expenses** incurred for the failure to prevent unauthorized access to, or use of, electronic or non-electronic data containing **Personal Information**.

26. Any of the following:

- a. The purchase or sale of or offer to purchase or sell any securities or any violation of the Securities Exchange Act of 1934 or the Securities Act of 1933 and any amendments thereto or any other foreign, federal, state or local statute, or any rule or regulation promulgated under such statutes, that regulates the offering, sale or purchase of securities.
- b. Any **Claim** brought by any security holder of the **Insured**, in their capacity as such, whether directly, by class action, or derivatively on behalf of the **Insured**.

27. Any **Claim** arising out of, caused by or related to a “Technology Errors & Omissions Wrongful Act.”

For purposes of this exclusion, the following definitions apply:

- a. “Technology Errors & Omissions Wrongful Act” means any negligent act, error or omission, including any negligent act, error or omission resulting in a breach of contract or in a failure of “Technology Products” to perform the function or serve the purpose intended by an **Insured** or by a person or entity for whom the **Insured** is legally liable, in the performance of “Technology Services.”
- b. “Technology Services” means the following services performed for others for compensation by an **Insured** or by any other person or entity for whom the **Insured** is legally liable:
 - i. analysis, design, integration, wiring, cabling, or conversion of computer and electronic technology systems or networks;
 - ii. designing, developing, programming, servicing, distributing, licensing, installing, maintaining and repairing computer software, computer code and computer firmware or hardware;
 - iii. education and training in the use of computer hardware or software;
 - iv. information services;
 - v. computer consulting;
 - vi. computer and network security services, including but not limited to providing content filtering, patch administration and security audits;
 - vii. internet services; or
 - viii. data processing in connection with any of the above listed services, including but not limited to storing, collecting, compiling, processing, mining, conversion, encryption, recording or analysis of data.
- c. “Technology Products” means any computer hardware, firmware, software, or related electronic product, equipment or device, specifically designed or intended for use in connection with any “Technology Services,” telecommunication systems or telecommunication service that is created, manufactured, developed, distributed, licensed, leased or sold by the **Insured** or for any **Insured** by others acting under the **Insured’s** trade name.

28. Any distribution or dissemination of unsolicited telemarketing, text messages, email, direct mail, facsimiles, or other communications, including but not limited to any violation of the Telephone Consumer Protection Act of 1991, the CAN-SPAM Act of 2003, or similar federal, state, local, or common law, if such distribution or dissemination is done by or on behalf of the **Insured**.

29. Any actual or alleged loss, transfer, theft, stealing, conversion, commingling, embezzlement, or misappropriation by any person of any kind of monies, funds, negotiable instruments, securities, property of any kind, or assets or any kind.

SECTION VI – CONDITIONS

1. Cancellation

- a. The first **Named Insured** shown in the Declarations may cancel this Policy by mailing or delivering to Us advance written notice of cancellation.
- b. We may cancel this Policy by mailing or delivering to the first **Named Insured** written notice of cancellation at least:
 - i. 10 days before the effective date of cancellation if We cancel for nonpayment of premium; or
 - ii. 30 days before the effective date of cancellation if We cancel for any other reason.
- c. We will mail or deliver Our notice to the first **Named Insured's** last mailing address known to Us.
- d. Notice of cancellation will state the effective date of cancellation. The **Policy Period** will end on that date.
- e. If this Policy is canceled, We will send the first **Named Insured** any premium refund due. If We cancel, the refund will be prorated. If the first **Named Insured** cancels, the refund may be less than pro rata. The cancellation will be effective even if We have not made or offered a refund.
- f. If notice is mailed, proof of mailing will be sufficient proof of notice.

2. Changes

This Policy contains all the agreements between You and Us concerning the insurance afforded. The first **Named Insured** shown in the Declarations is authorized to make changes in the terms of this Policy with Our written consent. This Policy's terms can be amended or waived only by endorsement issued by Us and made a part of this Policy.

3. Examination of Your Books and Records

We may examine and audit Your books and records as they relate to this Policy at any time during the **Policy Period** shown in the Declarations and up to three years afterward.

4. Inspections and Surveys

We have the right to i) make inspections and surveys at any time; ii) give You reports on the conditions We find; and iii) recommend changes.

We are not obligated to make any inspections, surveys, reports or recommendations, and any such actions We do undertake relate only to insurability and the premiums to be charged. We do not make safety inspections. We do not undertake to perform the duty of any person or organization to provide for the health or safety of workers or the public. And We do not warrant that conditions i) are safe or healthful; or ii) comply with laws, regulations, codes or standards.

Paragraph 2 of this condition applies not only to Us, but also to any rating, advisory, rate service or similar organization which makes insurance inspections, surveys, reports or recommendations.

5. Premiums

The first **Named Insured** shown in the Declarations: i) is responsible for the payments of all premiums; and ii) will be the payee for any return premiums We pay.

6. **Transfer of Your Rights and Duties Under This Policy**

Your rights and duties under this Policy may not be transferred without Our written consent, except in the case of death of an individual **Named Insured**.

If You are a sole proprietor and You die, Your rights and duties will be transferred to Your legal representative but only while acting within the scope of duties as Your legal representative. Until Your legal representative is appointed, anyone having proper temporary custody of Your property will have Your rights and duties but only with respect to that property.

7. **Subrogation**

With respect to any payment made under this Policy, We shall be subrogated to the **Insureds** rights of recovery to the extent of such payment. The **Insured** shall execute all papers required and shall do everything necessary to secure and preserve such rights, including the execution of such documents necessary to enable Us to bring suit in the **Insured's** name. Any recoveries, less the cost of obtaining them, will be distributed as follows:

- a. To You, until You are reimbursed for any **Loss** You sustain that exceed the sum of the Policy Limit of Insurance and the Deductible Amount, if any;
- b. Then to Us, until We are reimbursed for the payment made under this Policy; and
- c. Then to You, until You are reimbursed for that part of the payment equal to the Deductible Amount, if any.

8. **Bankruptcy**

Your bankruptcy, or the bankruptcy of Your estate if You are a sole proprietor, will not relieve Us of Our obligations under this Policy.

9. **Representations**

You represent that all information and statements contained in the **Application** are true, accurate and complete. All such information and statements are the basis for Our issuing this Policy. Misrepresentation of any material fact may be grounds for the rescission of this Policy.

10. **Changes in Exposure**

a. **Acquisition or Creation of Another Organization**

If before or during the **Policy Period**:

- i. You acquire securities or voting rights in another organization or create another organization which, as a result of such acquisition or creation, becomes a **Subsidiary**; or
- ii. You acquire any organization through merger or consolidation;

then such organization will be covered under this Policy as a **Subsidiary**, but only with respect to **Wrongful Acts** or **Loss** which occurred after the effective date of such acquisition or creation provided that the revenues of such entity do not exceed 20% of the **Named Insured's** annual revenues.

If the revenue of such entity exceeds 20% of the **Named Insured's** annual revenues, then coverage under this Policy will be afforded for a period of ninety (90) days, but only for **Claims**

arising out of **Wrongful Acts** first occurring after the entity becomes so owned. Coverage beyond such 90-day period will only be available if You:

- (1) give Us written notice of the acquisition or creation of such organization within ninety (90) days after the effective date of such action;
- (2) obtain Our written consent to extend the coverage provided by this Policy to such organization; and
- (3) upon obtaining Our consent, pay Us an additional premium, if necessary.

b. Acquisition of Named Insured

If during the **Policy Period**:

- i. the **Named Insured** merges into or consolidates with another organization, such that the **Named Insured** is not the surviving organization; or
- ii. another organization, or person or group of organizations and/or persons acting in concert, acquires securities or voting rights which result in ownership or voting control by the other organization(s) or person(s) of more than fifty percent (50%) of the outstanding securities or voting rights representing the present right to vote for the election of directors, trustees or managers (if a limited liability company) of the **Named Insured**;

then the coverage afforded under this Policy will continue until the end of the **Policy Period**, but only with respect to **Claims** arising out of **Wrongful Acts** which occurred prior to the effective date of such merger, consolidation or acquisition.

The **Named Insured** must give written notice of such merger, consolidation or acquisition to Us as soon as practicable, together with such information as We may reasonably require.

- c. If, before or during the **Policy Period**, an organization ceases to be a **Subsidiary**, the coverage afforded under this Policy with respect to such **Subsidiary** will continue until the end of the **Policy Period** but only with respect to **Claims** arising out of **Wrongful Acts** which occurred prior to the date such organization ceased to be a **Subsidiary**.

11. Other Insurance

If any covered **Claim** or **Loss** is insured by any other valid policy, then this Policy shall apply only in excess of the amount of any deductible, retention and limit applicable to such other insurance, whether such other policy is stated to be primary, contributory, excess, contingent or otherwise, unless such other policy is written specifically as excess over this Policy by reference in such other policy to this Policy's policy number.

When this Policy is excess, We shall have no duty under Insuring Agreement 6 – Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties to defend the **Insured** against any **Claim** or **Suit** if any other insurer has a duty to defend the **Insured** against that **Claim** or **Suit**.

If any covered **Claim** or **Loss** is insured by any other valid policy issued by Us, our liability under this Policy and such other policy combined shall not exceed the amount of the largest applicable Aggregate Limits or Sublimit(s) of Insurance.

12. Legal Action Against Us

No person or organization has a right: i) to join Us as a party or otherwise bring Us into a **Suit** asking for damages from an **Insured**; or ii) to sue Us under this Policy unless all of its terms have been fully complied with.

A person or organization may sue Us to recover on an agreed settlement or on a final judgment against an **Insured**, but We will not be liable for damages that are not payable under Insuring Agreement 6 – Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties, or that are in excess of the Policy Aggregate Limit of Insurance. An agreed settlement means a settlement and release of liability signed by Us, the first **Named Insured** and the claimant or the claimant's legal representative.

You may not bring any legal action against Us involving **Loss**: i) unless You have complied with all the terms of this Policy; ii) until ninety (90) days after You have filed proof of loss with Us; and iii) unless brought within two (2) years from the date You reported the **Loss** to Us.

If any limitation in this condition is prohibited by law, such limitation is amended so as to equal the minimum period of limitation provided by such law.

13. Separation of Insureds

Except with respect to the Policy Aggregate Limit of Insurance, and any rights or duties specifically assigned in Insuring Agreement 6 – Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties to the first **Named Insured**, this Policy applies separately to each **Insured** against whom a **Claim** is made.

14. Duties in the Event of Claim or Loss

After a situation that results in, or may result in, a **Loss** covered under this Policy is **Discovered**, You must notify Us in writing as soon as practicable, but not to exceed thirty (30) days from the date **Discovered**, and cooperate with Us in the investigation and settlement of the **Claim** or **Loss**. Additionally:

- a. Under Insuring Agreements 1 – Security Breach Response Expense, 2 – Extortion Threats, 3 – Recovery or Restoration of Electronic Data, 4 – Business Income and Extra Expense (Security Failure and System Failure), and 7 – Reputational Harm You must:
 - i. notify local law enforcement officials; and
 - ii. submit to examination under oath at Our request and give Us a signed statement of Your answers; and
 - iii. provide Us with a detailed, sworn proof of loss within one hundred twenty (120) days. The provision of a sworn proof of loss within one hundred twenty (120) days is a condition precedent to coverage under this Policy.

In addition, under Insuring Agreement 2 – Extortion Threats, You must also:

- (1) determine that the **Extortion Threat** has actually occurred; and
 - (2) with respect to **Ransomware**, make every reasonable effort to access Your **Electronic Data** from backup, if any, and to remediate the cause of the **Ransomware**; and
 - (3) make every reasonable effort to immediately notify Us before making any ransom payment based upon the **Extortion Threat**; and
 - (4) approve any ransom payment based upon the **Extortion Threat**.
- b. Under Insuring Agreement 6 – Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties, You must:
 - i. immediately record the specifics of the **Claim** and the date **Discovered**; and
 - ii. immediately send Us copies of any demands, notices, summonses or legal papers received in connection with the **Claims**; and
 - iii. authorize Us to obtain records and other information; and
 - iv. assist Us, upon Our request, in the enforcement of any right against any person or organization which may be liable to You because of a **Loss** to which this Policy may also apply.

You will not, except at Your own cost, voluntarily make a payment, assume any obligation or incur any expense without Our consent.

15. Extended Reporting Periods

a. Automatic Extended Reporting Period

If the **Named Insured** cancels or non-renews this Policy, the Insurer cancels or non-renews this Policy, or if there is a decrease in limits, reduction of coverage, increased deductible or self-insured retention, new exclusion, or any other change less favorable to the **Insured**, then the **Insured** will have an automatic, non-cancelable 60-day **Extended Reporting Period**.

b. Supplemental Extended Reporting Period

If the **Named Insured** cancels or non-renews this Policy, the Insurer cancels or non-renews this Policy, or if there is a decrease in limits, reduction of coverage, increased deductible or self-insured retention, new exclusion, or any other change less favorable to the **Insured**, the **Named Insured** will have the right to purchase an optional **Extended Reporting Period** of up to three (3) years to immediately follow the automatic **Extended Reporting Period**.

The optional **Extended Reporting Periods** and their respective additional premiums are stated in the Declarations or by endorsement. The premium for such **Extended Reporting Period** is based on the rating of the canceled or terminated Policy. We must receive written notice of the optional **Extended Reporting Period** elected together with payment of the applicable additional premium, within either 1) sixty (60) days after the end of the Policy Period or 2) thirty (30) days from the effective date of mailing or deliver of the notification advising You of the availability of, the premium for, and the importance of purchasing optional **Extended Reporting Period**. If the Insurer does not receive payment within such period, the **Insurer** will not be required to provide any optional **Extended Reporting Period**.

If an optional **Extended Reporting Period** is purchased, we will provide an Additional Extended Reporting Period Additional Limit of Insurance equal to the remaining applicable Limit of Insurance of the canceled or terminated Policy.

16. Valuation – Settlement

All premiums, limit(s) of insurance, deductible amounts, **Loss** and any other monetary amounts under this Policy are expressed and payable in the currency of the United States of America. If judgment is rendered, settlement is agreed to or another component of **Loss** under this Policy is expressed in any currency other than United States of America dollars, payment under this Policy shall be made in United States dollars at the rate of exchange published in The Wall Street Journal on the date the final judgment is entered, settlement amount is agreed upon or the other component of **Loss** is due, respectively.

- a. With respect to **Loss** covered under Insuring Agreement 4 – Business Income and Extra Expense (Security Failure and System Failure), the amount of “business income” will be determined based on consideration of:
- i. the net income (net profit or loss before income taxes) earned from your business operations before the **Interruption** occurred;
 - ii. the likely net income (net profit or loss before income taxes) that would have been earned or incurred by your business operations if no **Interruption** had occurred, but not including any net income that would likely have been earned as a result of an increase in the volume of business due to favorable business conditions caused by the impact of the **Cyber Incident** on customers or on other businesses;

- iii. the continuing normal operating expenses, including payroll, necessary to resume Your business operations with the same quality of service that existed before the **Interruption**; and
 - iv. other relevant sources of information, including Your financial records and accounting procedures, bills, invoices and other vouchers, and debts, liens and contracts.
- b. With respect to **Loss** covered under Insuring Agreement 4 – Business Income and Extra Expense (Security Failure and System Failure), the amount of “extra expense” will be determined based on:
- i. necessary and reasonable expenses incurred during an Interruption that exceed the normal operating expenses that would have been incurred if no **Interruption** had occurred. We will deduct from the total of such expenses the salvage value that remains of any property bought for temporary use during the period of coverage once Your business operations are resumed; and
 - ii. necessary and reasonable expenses that reduce the “business income” **Loss** that otherwise would have been incurred during the **Interruption**.
- c. With respect to **Loss** covered under Insuring Agreement 7 – Reputational Harm, due consideration will be given to:
- i. Your business operations prior to the first publication of any **Adverse Publication**;
 - ii. the public and market perception of the Insured prior to the first publication of any **Adverse Publication**;
 - iii. Your net profit or net loss during the twelve (12) months immediately preceding the publication of the **Adverse Publication**;
 - iv. any amounts made up during, or within a reasonable time after the end of, the **Reputational Harm Indemnity Period**; and
 - v. market and industry trends, variations, and circumstances, including seasonable influences and economic conditions, which would have affected Your business operations regardless of the **Adverse Publication**.

17. Confidentiality

Under Insuring Agreement 2 – Extortion Threats, **Insureds** must make every reasonable effort not to divulge the existence of this coverage.

18. Territory

This Policy covers **Wrongful Acts, Security Breaches, Cyber Incidents** and **Extortion Threats** which occur anywhere in the world. However, this Policy only covers **Suits** brought in the United States of America (including its territories and possessions).

19. Policy Bridge – Discovery Replacing Loss Sustained

If this Policy replaces insurance that provided You with an extended period of time after cancellation or nonrenewal in which to **Discover Loss** resulting directly from any **Cyber Incident, Extortion Threat, Security Breach**, or **Claim** and which did not terminate when this Policy became effective:

We will not pay for any **Loss** resulting directly from any **Cyber Incident, Extortion Threat, Security Breach**, or **Claim** that occurred during the Policy Period of that prior insurance which is **Discovered** during such extended period of time, unless the amount of that **Loss** exceeds the Limit of Insurance and Deductible Amount of that prior insurance. In that case, We will pay for the excess **Loss** subject to the terms and conditions of this Policy.

Condition 11 – Other Insurance does not apply to this condition.

20. Nonrenewal

We may non-renew this Policy for any reason allowable by applicable law. If We decide not to renew this Policy, We will mail or deliver to the first **Named Insured** written notice of the nonrenewal not less than thirty (30) days before the expiration date.

If notice is mailed, proof of mailing will be sufficient proof of notice.

SECTION VII – DEFINITIONS

1. **Adverse Publication** means a publication by a third part of any media, including but not limited to, television, print media, radio or electronic networks, the internet, or e-mail, to the general public that states or alleges the Insured has experienced a **Cyber Incident**, **Extortion Threat**, or **Security Breach**.

2. **AI Related Cyber Event** means;

- a. The unauthorized access to, or use of, electronic data within a **Computer System**;
- b. A **Cyber Incident**; or
- c. A **Security Breach**;

resulting directly from the use of any artificial intelligence technology, including through the use of machine learning or prompt injection points.

3. **Application** means the signed application for this Policy, including any attachments, attestations, and other materials submitted in conjunction with the signed application, digital or otherwise.

4. **Card Company** means American Express, Discover Financial Services, JCB International, MasterCard Worldwide, Visa Inc. or any other credit card company that requires its merchants to adhere to the Payment Card Industry (PCI) Data Security Standards.

5. **Claim** means:

- a. A written demand for monetary or nonmonetary damages, including but not limited to injunctive relief;
- b. A civil proceeding commenced by the service of a complaint or similar proceeding;
- c. Under Paragraph b. of Insuring Agreement 6 – Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties, a **Regulatory Proceeding** commenced by the filing of a notice of charges, formal investigative order, service of summons or similar document; or
- d. Under Paragraph c. of Insuring Agreement 6 – Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties an action brought by a **Card Company** of the Payment Card Industry (PCI);

against any **Insured** for a **Wrongful Act**, including any appeal therefrom.

6. **Computer System** means any computer, including transportable or handheld devices, electronic storage devices and related peripheral components; any systems and applications software, or any related telecommunications networks connected to or used in connection with such computer or devices: i) which collects, transmits, processes, stores or retrieves Your **Electronic Data**; and ii) which is:

- a. Owned by You;
- b. Leased by You and operated by any **Insured**;

- c. Owned and operated by an **Employee** who has agreed in writing to Your personal device use policy; or
- d. Operated by an authorized **Third Party**, but only with respect to Your **Electronic Data**.

7. **Cyber Incident** means:

- a. Any i) **Hacker** attack; ii) malicious code; or iii) **Virus** that is directed at, enacted upon or introduced into a **Computer System** (including Your **Electronic Data**) and is designed to access, alter, corrupt, damage, delete, destroy, disrupt, encrypt, use or prevent or restrict access to or the use of any part of a **Computer System** (including Your **Electronic Data**) or otherwise disrupt its normal functioning or operation.

Recurrence of the same **Virus** after a **Computer System** has been restored shall constitute a separate **Cyber Incident**.

- b. Any denial of service attack specifically directed at You which disrupts, prevents or restricts access to or use of a **Computer System** or otherwise disrupts the normal functioning or operation of a **Computer System**.
- c. Any **AI Related Cyber Event**.

8. **Discovery** or **Discovered** means the time when any **Employee** who is a Chief Executive Officer, Chief Financial Officer, Chief Security Officer, Chief Technology Officer, Chief Information Officer, Risk Manager, General Counsel, owner, general manager, or any functionally equivalent positions of the **Insured** or any **Subsidiary**, regardless of title first becomes aware of facts which would cause a reasonable person to believe that a **Loss** covered by this Policy has been or will be incurred, regardless of when the act or acts causing or contributing to such **Loss** occurred, even though the exact amount or details of **Loss** may not then be known.

Discovery or **Discovered** also means the time when any **Insured** first receives notice of an actual or potential **Claim** in which it is alleged that You are liable to a third party under circumstances which, if true, would constitute a **Loss** under this Policy.

9. **Electronic Data** means information, facts, images or sounds stored as or on, created or used on, or transmitted to or from computer software (including systems and applications software) on electronic storage devices including, but not limited to, hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment. **Electronic Data** is not tangible property.

Electronic Data does not include Your **Electronic Data** that is licensed, leased, rented or loaned to others.

10. **Employee** means any natural person who was, now is, or will be:

- a. Employed on a full- or part-time basis;
- b. Furnished temporarily to You to substitute for a permanent employee on leave or to meet seasonal or short-term workload conditions;
- c. Leased to You by a labor leasing firm under an agreement between You and the labor leasing firm to perform duties related to the conduct of Your business but does not mean a temporary employee as defined in Paragraph 9.b. above;
- d. An officer;
- e. A director, trustee or manager (if a limited liability company);
- f. A volunteer worker;
- g. A partner or member (if a limited liability company); or
- h. An **Independent Contractor**,

of the **Named Insured** and those of any organization qualifying as a **Subsidiary** under the terms of this Policy, but only while acting within the scope of their duties as determined by the **Named Insured** or such **Subsidiary**.

11. **Extended Reporting Period** means a designated period immediately following cancellation, nonrenewal, decrease in limits, reduced coverage, increased deductible or self-insured retention, newly added exclusions, or any other changes which are less favorable to the **Insured** of the Policy, during which **Claims** first made against the **Insured** will be deemed made during the **Policy Period**, but only for **Wrongful Acts** or **Interrelated Wrongful Acts** that first occurred on or after the Retroactive Date, if any, listed on the Declarations, and prior to the effective date of cancellation, nonrenewal, decrease in limits, reduced coverage, increased deductible or self-insured retention, newly added exclusions, or any other changes which are less favorable to the **Insured**, of the Policy.
12. **Extortion Threat** means a threat or series of related threats:
- a. To perpetrate a **Cyber Incident**;
 - b. To disseminate, divulge or utilize: i) Your proprietary information; or ii) weakness in the source code within a **Computer System** by gaining unauthorized access to a **Computer System**;
 - c. To destroy, corrupt or prevent normal access to a **Computer System** (including Your **Electronic Data**) by gaining or having gained unauthorized access to a **Computer System**;
 - d. To inflict **Ransomware** on a **Computer System**; or
 - e. To publish Your client's or **Employee's Personal Information**.

Extortion Threat does not include a threat or series of threats to any **Third Party**.

13. **Hacker** means a person who accesses a **Computer System** (including Your **Electronic Data**) who is: i) not authorized to have such access; or ii) authorized to have such access but who uses such access in an unauthorized manner.
14. **Independent Contractor** means any person or entity contracted by the **Named Insured** to perform the same business operations as the **Named Insured**, but only while in the course of their performance of such business operations on behalf of, or at the direction of, the **Named Insured**.
15. **Insured** means any **Named Insured** and its **Employees**.
16. **Interrelated Wrongful Acts** means all **Wrongful Acts** that have as a common nexus any: i) fact, circumstance, situation, event, transaction or cause; or ii) a series of casually connected facts, circumstances, situations, events, transactions or causes.
17. **Interruption** means:
- a. With respect to a **Cyber Incident**:
 - i. an unanticipated cessation or slowdown of Your business operations; or
 - ii. Your voluntary suspension of Your business operations for the purpose of avoiding or mitigating the possibility of transmitting a **Virus** or malicious code to another person or organization;

and, with regard to Paragraphs a.i and a.ii. above, shall be deemed to begin when Your business operations are interrupted and ends at the earliest of:

- (1) one hundred-eighty (180) days after the **Interruption** begins;
- (2) the time when Your business operations are resumed; or
- (3) the time when service is restored to You.

- b. With respect to an **Extortion Threat**, Your voluntary suspension of Your business operations:
- i. based upon clear evidence of a credible threat; or
 - ii. based upon the recommendation of a security firm, if any;
- and, with regard to Paragraphs b.i and b.ii. above, shall be deemed to begin when Your business operations are interrupted and ends at the earliest of:
- (1) one hundred-eighty (180) days after the **Interruption** begins;
 - (2) the time when Your business operations are resumed; or
 - (3) the time when service is restored to You.
- c. With respect to a **System Failure**:
- i. an unanticipated cessation or slowdown of Your business operations; or
 - ii. Your voluntary suspension of Your business operations,
- resulting directly from a **System Failure** of Your **Computer System**;
- and, with regard to Paragraphs i and ii. above, shall be deemed to begin when Your business operations are interrupted and ends at the earliest of:
- (1) one hundred-eighty (180) days after the **Interruption** begins;
 - (2) the time when Your business operations are resumed; or
 - (3) the time when service is restored to You.
18. **Loss** means the definitions set forth in each of the respective Insuring Agreements of this Policy.
19. **Money** means currency, coins or bank notes in current use and having a face value, travelers' checks, register checks and money orders held for sale to the public. The term Money does not include digital currency or other negotiable and nonnegotiable instruments or contracts representing either Money or property.
20. **Named Insured** means the entity or entities shown in the Declarations and any **Subsidiary**.
21. **Personal Information** means any information not available to the general public for any reason through which an individual may be identified including, but not limited to, an individual's:
- a. Social security number, driver's license number or state identification number;
 - b. Protected health information;
 - c. Financial account numbers;
 - d. Security codes, passwords, PINs associated with credit, debit or charge card numbers which would permit access to financial accounts; or
 - e. Any other nonpublic information as defined in **Privacy Regulations**.
22. **Policy Period** means the period of time from the inception date of this Policy shown in the Declarations to the expiration date shown in the Declarations, or its earlier cancellation or termination date, and specifically excludes any **Extended Reporting Period**.
23. **Pollutants** means any solid, liquid, gaseous or thermal irritant or contaminant, including smoke, vapor, soot, fumes, acids, alkalis, chemicals and waste. Waste includes materials to be recycled, reconditioned or reclaimed.

24. **Privacy Regulations** means any of the following statutes and regulations, and their amendments, associated with the control and use of personally identifiable financial, health or other sensitive information including, but not limited to:
- a. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191);
 - b. The Health Information Technology for Economic and Clinical Health Act (HITECH) (American Recovery and Reinvestment Act of 2009);
 - c. The Gramm-Leach-Bliley Act of 1999;
 - d. Section 5(a) of the Federal Trade Commission Act (15 U.S.C. 45(a)), but solely for alleged unfair or deceptive acts or practices in or affecting commerce;
 - e. The Identity Theft Red Flags Rules under the Fair and Accurate Credit Transactions Act of 2003; or
 - f. Any other similar local, state, federal or foreign identity theft or privacy protection statute or regulation.
25. **Ransomware** means any software that is used to demand a ransom payment by: i) restricting access to a **Computer System**; or ii) encrypting Your **Electronic Data** held within a **Computer System**.
26. **Ransom Demand** means a demand by a third-party actor communicated in an electronic format to You as a request for payment in any form, including virtual currency, to rectify an **Extortion Threat** that is **Discovered** during the **Policy Period**.
27. **Ransom Payment** means a monetary payment made during the **Policy Period** in any form, including virtual currency, to a third-party actor with Our prior written consent to resolve an **Extortion Threat**.
28. **Reputational Harm Indemnity Period** means the period beginning on the date the **Adverse Publication** is first published and ends after the earlier of:
- a. one hundred-eighty (180) days; or
 - b. the date that the Insured's gross revenues are restored to the level they would have been but for the Adverse Publication.
29. **Security Breach** means a privacy breach that includes the acquisition, access, theft, or disclosure of **Personal Information** held within a **Computer System** or in non-electronic form at or while in the care, custody or control of the **Insured** or authorized **Third Party** by a person: i) not authorized to have access to such information; or ii) authorized to have access to such information but whose access results in the unauthorized disclosure of such information; or iii) resulting from an **AI Related Cyber Event**.
30. **Securities** mean negotiable and non-negotiable instruments or contracts representing either Money or property.
- Securities** does not include **Money**.
31. **Subsidiary** means any organization in which more than fifty percent (50%) of the outstanding securities or voting rights representing the present right to vote for the election of directors, trustees, managers (if a limited liability company) or persons serving in a similar capacity is owned, in any combination, by one or more **Named Insureds**.
32. **Suit** means a civil proceeding in which damages to which this Policy applies are claimed against the **Insured**. **Suit** includes:
- a. An arbitration proceeding in which such damages are claimed and to which the **Insured** submits with Our consent; or
 - b. Any other alternative dispute resolution proceeding in which such damages are claimed and to which the **Insured** submits with Our consent.

Suit does not include a civil proceeding seeking recognition and/or enforcement of a foreign money judgment.

33. **System Failure** means any sudden, unintentional, or unexpected and continuous outage, degradation or failure of a **Computer System** which disrupts, prevents, or restricts the normal functioning of Your business operations which would otherwise have been handled in whole or in part by the **Computer System** and is directly caused by a malfunction in normal computer function or network service, or hardware failure.

System Failure does not include:

- a. Failure of hardware or software due to product defects or design/manufacturing flaws, ordinary wear and tear of physical components, or use of hardware past End of Life Announcements (EOLA) or Last Date of Support (LODS);
- b. Failure of a **Computer System** operated by a **Third Party** which results in an extended outage beyond the services performed for you by the **Third Party**;
- c. Failure to adequately anticipate or capacity plan for expected and/or above-normal operational demand for a **Computer Systems**. However, this exclusion shall not apply if such operational demand is caused by a denial of service attack;
- d. Failure to renew any domain names or uniform resource locators;
- e. Failure of a **Computer System** caused by a **Cyber Incident**; or
- f. Voluntary suspension or shutdown of a **Computer System** operated by a **Third Party**.

34. **Third Party** means any entity that You engage under the terms of a written contract to perform services for You.

35. **Virus** means any kind of malicious code designed to damage or destroy any part of a **Computer System** (including Your **Electronic Data**) or disrupt its normal functioning.

36. **Wrongful Act** means any actual or alleged:

- a. **Security Breach**;
- b. Failure to prevent unauthorized access to, or use of, electronic or non-electronic data containing **Personal Information**;
- c. Failure to prevent the transmission of a **Virus** through a **Computer System** into a computer network, any application software, or a computer operating system or related network that is not rented, owned, leased by, licensed to or under the direct operational control of the **Insured**; or
- d. Failure to provide notification of any actual or potential **Security Breach** if such notification is required by any Security breach notification law;

by, or asserted against, an **Insured**.

Policy Number:

Issued Date:

Effective Date:

SIGNATURE PAGE

In Witness Whereof, we have caused this policy to be executed and attested, and, if required by state law, this policy shall not be valid unless countersigned by our authorized representative.

Juliette Song

(signature)

Juliette Song -
Secretary

Torben Ostergaard

(signature)

Torben Ostergaard -
President

SPECIMEN

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

TRADE OR ECONOMIC SANCTIONS

This endorsement modifies insurance provided under the following:

COMMERCIAL CYBER INSURANCE POLICY

This insurance does not provide any coverage, and We shall not make payment of any claim or provide any benefit hereunder, to the extent that the provision of such coverage, payment of such claim or provision of such benefit would expose us to a violation of any applicable trade or economic sanctions, laws or regulations, including but not limited to those administered and enforced by the United States Treasury Department's Office of Foreign Assets Control (OFAC).

All other terms and conditions remain unchanged.

SPECIMEN

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

ADDITIONAL INSURED – DESIGNATED PERSON OR ORGANIZATION

This endorsement modifies insurance provided under the following:
COMMERCIAL CYBER INSURANCE POLICY

ADDITIONAL INSURED SCHEDULE

Name of Additional Insured Person(s) or Organization(s):
Information required to complete this Schedule, if not shown above, will be shown in the Declarations.

The following applies with respect to the Insuring Agreement(s) selected in the Schedule:

- I. With respect to the insurance afforded to the additional **Insured(s)** shown in the Schedule, the following is added to **SECTION II – LIMITS OF INSURANCE**:

If coverage provided to the additional **Insured(s)** is required by a contract or agreement, the most We will pay on behalf of the additional **Insured(s)** is the amount:

1. Required by the contract or agreement; or
2. Available under the applicable Aggregate Limit(s) of Insurance shown in the Declarations; whichever amount is less.

This endorsement shall not increase the applicable Aggregate Limit(s) of Insurance shown in the Declarations.

However, the insurance afforded to such additional **Insured(s)** only applies to the extent permitted by law.

- II. The definition of **Insured** in **SECTION VII – DEFINITIONS** is deleted in its entirety and replaced with the following:

Insured means any **Named Insured** and its **Employees**.

Solely with respect to SECTION 1 – INSURING AGREEMENTS, 6. **Security Breach Liability** Including Payment Card Industry (PCI) Fines and Penalties, **Insured** also means the person(s) or organization(s) shown in the Additional Insured Schedule, but only with respect to liability for **Loss** and **Defense Expenses** resulting from a **Wrongful Act** or a series of **Interrelated Wrongful Acts** committed, in whole or in part, by You or those acting on Your behalf.

All other terms and conditions remain unchanged.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

INVOICE MANIPULATION ENDORSEMENT

Invoice Manipulation Coverage Limit: \$
Invoice Manipulation Deductible: \$

This endorsement modifies insurance provided under the following:

COMMERCIAL CYBER INSURANCE POLICY

Unless modified by this Invoice Manipulation Endorsement, all provisions of the Policy to which this endorsement is attached, as well as all terms and conditions, remain unchanged and applicable.

In consideration of the premium charged for the Policy, it is hereby understood and agreed that:

I. The following Insuring Agreement is added to SECTION I – INSURING AGREEMENTS:

Invoice Manipulation:

Subject to the Invoice Manipulation Coverage Limit and Deductible set forth above, We will pay for a **Invoice Manipulation Loss** resulting directly from a **Invoice Manipulation Event** that is first **Discovered** during the Policy Period and reported in accordance with Condition 14. **Duties in the Event of Claim or Loss** in **SECTION VI – CONDITIONS**.

With respect to this Invoice Manipulation Insuring Agreement:

- a. **Client** means any person or entity with whom You have entered into a written contract to provide services or deliverables.
- b. **Money** means currency, coins or banknotes in current use and having a face value, travelers' checks, register checks and money orders held for sale to the public. The term **Money** does not include digital currency or other negotiable and nonnegotiable instruments or contracts representing either **Money** or property.
- c. **Invoice Manipulation Event** means the intentional use of Your **Computer System** by a person or organization that is not an **Insured** to mislead or deceive Your **Client** or **Vendor** into transferring **Money** intended for You to another person or entity.
- d. **Invoice Manipulation Loss** means the loss of **Money** as a result of a **Invoice Manipulation Event**.
- e. **Vendor** means any person or entity with whom You have entered into a written contract to provide services to You provided that entity is not owned, operated or controlled by You. **Vendor** does not include any financial institutions with which you directly or indirectly do business.

II. The following is added to SECTION II – LIMITS OF INSURANCE, 2. Aggregate Sublimit(s) of Insurance:

The most We will pay for all Loss covered under the Invoice Manipulation Insuring Agreement is the Invoice Manipulation Aggregate Sublimit of Insurance, if any, shown above, which is part of,

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

not in addition to the Policy Aggregate Limit of Insurance set forth on the Declarations to this Policy. Any such Aggregate Sublimit(s) of Insurance shall be reduced by the amount of any payment for **Loss** under the Insuring Agreement to which such Aggregate Sublimit of Insurance applies. Upon exhaustion of any Aggregate Sublimit of Insurance by such payments, We will have no further obligations or liability of any kind with respect to **Loss** subject to such Sublimit of Insurance.

III. The following is added to SECTION III - DEDUCTIBLE

Under the Invoice Manipulation Insuring Agreement, We will pay only the amount of **Loss** which is in excess of the Invoice Manipulation Deductible amount shown above.

All other terms and conditions remain unchanged.

SPECIMEN

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

TELECOMMUNICATIONS FRAUD ENDORSEMENT

Telecommunications Fraud Coverage Limit:

This endorsement modifies insurance provided under the following:

COMMERCIAL CYBER INSURANCE POLICY

Unless modified by this Telecommunications Fraud Endorsement, all provisions of the Policy to which this endorsement is attached, as well as all terms and conditions, remain unchanged and applicable.

This endorsement extends certain coverages. The headers in this endorsement are only for convenience. Read the entire policy carefully to determine rights, duties and what is and is not covered.

In consideration of the premium charged for the Policy, it is hereby understood and agreed that:

I. The following Insuring Agreement is added to SECTION I – INSURING AGREEMENTS:

Telecommunications Fraud:

Subject to the Telecommunications Fraud Coverage Limit set forth above and any Deductible specified in the Declarations to this policy, We will pay for any monetary **Loss** sustained by **You**, including but not limited to phone bills, first **Discovered** during the Policy Period and reported in accordance Condition **14. Duties in the Event of Claim or Loss** in **SECTION VI - CONDITIONS**, directly resulting from an intentional unauthorized access to Your **Telephone System** by a third party.

With respect to this Telecommunications Fraud Insuring Agreement:

a. **Loss** solely means the monetary cost of unauthorized calls or unauthorized use of **Your Telephone System's** bandwidth.

b. **Telephone System** means the VoIP phone system directly under **Your** control.

II. The following is added to SECTION II – LIMITS OF INSURANCE, 2. Aggregate Sublimit(s) of Insurance:

The most We will pay for all Loss covered under the Telecommunications Fraud Insuring Agreement is the Telecommunications Fraud Aggregate Sublimit of Insurance, if any, shown above or in the Declarations., which are part of, and not in addition to, the Policy Aggregate Limit of Insurance. Upon exhaustion of any Aggregate Sublimit of Insurance by such payments, We will have no further obligations of liability of any kind with respect to **Loss** subject to such Sublimit of Insurance.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

III. The following is added to **SECTION III – DEDUCTIBLE**

Under the Telecommunications Fraud Insuring Agreement, We will pay only the amount of **Loss** which is in excess of the Policy Deductible shown in the Declarations.

All other terms and conditions remain unchanged.

SPECIMEN

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

HARDWARE REPLACEMENT AND BRICKING COSTS ENDORSEMENT

Hardware Replacement and Bricking Costs Coverage Limit: \$

This endorsement modifies insurance provided under the following:

COMMERCIAL CYBER INSURANCE POLICY

Unless modified by this Hardware Replacement and Bricking Costs Endorsement, all provisions of the Policy to which this endorsement is attached, as all terms and conditions, remain unchanged and applicable.

In consideration of the premium charged for the Policy, it is hereby understood and agreed that:

I. The following Insuring Agreement is added to **SECTION I – INSURING AGREEMENTS**:

Hardware Replacement and Bricking Costs

Subject to the Hardware Replacement and Bricking Costs Coverage Limit set forth above and any Deductible specified in the Declarations to this policy, We will pay for **Loss** directly resulting from a **Cyber Incident** first **Discovered** during the Policy Period and reported in accordance with Condition **14. Duties in the Event of Claim or Loss** in **SECTION VI – CONDITIONS**, to mitigate the potential of a future **Cyber Incident** or **Security Breach**.

With respect to this Hardware Replacement and Bricking Costs Insuring Agreement:

a. Loss means the cost to replace hardware, including but not limited to, computers or any associated devices or equipment operated by, and either owned by or leased to, the **Insured** that are unable to function as intended due to corruption or destruction of software or firmware.

b. Loss does not include any sums related to labor costs associated with installing, connecting or setting up the hardware.

II. The following is added to **SECTION II – LIMITS OF INSURANCE, 2. Aggregate Sublimit(s) of Insurance**:

The most We will pay for all Loss covered under the Hardware Replacement and Bricking Costs Insuring Agreement is the Hardware Replacement and Bricking Costs Aggregate Sublimit of Insurance, if any, shown above or in the Declarations, which are part of, and not in addition to, the Policy Aggregate Limit of Insurance. Upon exhaustion of any Aggregate Sublimit of Insurance by such payments, We will have no further obligations of liability of any kind with respect to **Loss** subject to such Sublimit of Insurance.

III. The following is added to **SECTION III – DEDUCTIBLE**:

Under the Hardware Replacement and Bricking Costs Insuring Agreement, We will pay only the amount of **Loss** which is in excess of the Policy Deductible shown in the Declarations.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

IV. Exclusion 4 in **SECTION V – EXCLUSIONS** is deleted in its entirety and replaced with the following:

Bodily Injury

Bodily Injury means bodily injury, sickness or disease sustained by a person, including death resulting from any of these at any time. It also means mental injury, mental anguish, mental tension, emotional distress, pain or suffering or shock sustained by any person.

However, this exclusion will not apply to any mental anguish or emotional distress which gives rise to a **Claim** or **Loss** covered under Insuring Agreement 6 – Security Breach Liability Including Payment Card Industry (PCI) Fines and Penalties.

All other terms and conditions remain unchanged.

SPECIMEN

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

WEBSITE MEDIA CONTENT LIABILITY ENDORSEMENT

**Website Media Content Liability Coverage Limit:
Website Media Content Liability Deductible:**

This endorsement modifies insurance provided under the following:
COMMERCIAL CYBER INSURANCE POLICY

Unless modified by this Website Media Content Liability Endorsement, all provisions of the Policy to which this endorsement is attached, as well as all terms and conditions, remain unchanged and applicable.

In consideration of the premium charged for the Policy, it is hereby understood and agreed that:

I. The following Insuring Agreement is added to **SECTION I – INSURING AGREEMENTS**:

Website Media Content Liability

Subject to the Website Media Content Liability Coverage Limit and Deductible set forth above, We will pay for **Loss** that the Insured becomes legally obligated to pay and **Defense Expenses** as a result of a **Claim** that is **Discovered** during the Policy Period and reported in accordance with Condition **14. Duties in the Event of Claim or Loss** in **SECTION VI – CONDITIONS**, for one or more of the following acts first committed on or after the retroactive date and before the end of the Policy Period in the course of Your display of **Media Material** on Your website or on social media web pages created and maintained by or on behalf of You:

- a. invasion of or interference with an individual's right of publicity, including commercial appropriation of name, persona, voice or likeness; or
- b. plagiarism, piracy or misappropriation of ideas under implied contract; or
- c. infringement of copyright; or
- d. infringement of domain name, trademark, trade name, trade dress, logo, title, metatag, slogan, service mark, service name; or
- e. improper deep-linking or framing within electronic content.

With respect to this Website Media Content Liability Insuring Agreement:

- a. **Media Material** means any information in electronic form, including words, sounds, numbers, images, or graphics and shall also include advertising, video, streaming content, webcasting, online forums, bulletin boards and chat room content, but does not mean computer software or the actual goods, products or services described, illustrated or displayed in such **Media Material**.

II. Exclusions Applicable to the Website Media Content Liability Insuring Agreement:

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

We will not be liable for any **Claim** resulting from an act based upon, attributable to or arising out of:

1. An actual or alleged infringement of, violation of, misappropriation of or assertion of any right to or interest in any:
 - a. Patent, copyright, trademark, trade dress, certification mark, collective mark, service mark, expression, idea, likeness, name, slogan, style of doing business, symbol, title, trade secret or other intellectual property right by or on behalf of any **Insured**, provided that this Exclusion does not apply to a claim resulting from an act based upon, attributable to or arising out of infringement of copyright, or infringement of domain name, trademark, trade name, trade dress, logo, title, metatag, slogan, service mark, service name in the course of Your display of **Media Material** on Your website or on social media web pages created and maintained by or on behalf of You; or
 - b. Software or computer code or its source content or material by or on behalf of any **Insured**.

III. The following is added to **SECTION II – LIMITS OF INSURANCE, 2. Aggregate Sublimit(s) of Insurance:**

The most We will pay for all Loss covered under the Website Media Content Liability Insuring Agreement is the Website Media Content Liability Sublimit of Insurance shown above, which is part of, not in addition to the Policy Aggregate Limit of Insurance set forth in the Declarations to this Policy. Upon exhaustion of any Aggregate Sublimit of Insurance by such payments, We will have no further obligations or liability of any kind with respect to **Loss** subject to such Sublimit of Insurance.

All other terms and conditions remain unchanged.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

POST BREACH REMEDIATION COVERAGE ENDORSEMENT

Post Breach Remediation Coverage Limit:

This endorsement modifies insurance provided under the following:

COMMERCIAL CYBER INSURANCE POLICY

Unless modified by this Post Breach Remediation Coverage Endorsement, all provisions of the Policy to which this endorsement is attached, as well as all terms and conditions, remain unchanged and applicable.

This endorsement extends certain coverages. The headers in this endorsement are only for convenience. Read the entire policy carefully to determine rights, duties and what is and is not covered.

In consideration of the premium charged for the Policy, it is hereby understood and agreed that:

I. The following Insuring Agreement is added to **SECTION I – INSURING AGREEMENTS:**

Post Breach Remediation:

Subject to the Post Breach Remediation Coverage Limit set forth above and any Deductible specified in the Declarations to this policy, We will pay **Loss** incurred with **Our** prior written approval during the Policy Period and reported in accordance with Condition **14. Duties in the Event of Claim or Loss** in **SECTION VI – CONDITIONS**, to resolve any vulnerabilities or weaknesses in your **Computer System** that are identified by an independent security firm after a **Cyber Incident** or **Security Breach**. The upgrades or improvements must be determined by the independent security firm to reduce the probability or potential damage from a **Cyber Incident** or **Security Breach** in the future.

With respect to this Post Breach Remediation Insuring Agreement:

a. **Loss** solely means:

- i. labor costs incurred by an independent security firm to determine whether any vulnerabilities or weaknesses exist in Your **Computer System** that are identified by an independent security firm after a **Cyber Incident** or **Security Breach**; and
- ii. labor costs incurred to resolve any vulnerabilities or weaknesses in your **Computer System** that are identified by an independent security firm after a **Cyber Incident** or **Security Breach**.

II. The following is added to **SECTION II – LIMITS OF INSURANCE. 2. Aggregate Sublimit(s) of Insurance:**

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

The most We will pay for all Loss covered under the Post Breach Remediation Insuring Agreement is the Post Breach Remediation Aggregate Sublimit of Insurance, if any, shown above or in the Declarations, which are part of, and not in addition to, the Policy Aggregate Limit of Insurance. Upon exhaustion of any Aggregate Sublimit of Insurance by such payments, We will have no further obligations of liability of any kind with respect to **Loss** subject to such Sublimit of Insurance.

III. The following is added to **SECTION III – DEDUCTIBLE:**

Under the Post Breach Remediation Insuring Agreement, We will pay only the amount of **Loss** which is in excess of the Policy Deductible amount shown in the Declarations.

All other terms and conditions remain unchanged.

SPECIMEN

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

SERVICE FRAUD INCLUDING CRYPTOJACKING ENDORSEMENT

Service Fraud Coverage Limit:

This endorsement modifies insurance provided under the following:

COMMERCIAL CYBER INSURANCE POLICY

Unless modified by this Service Fraud Endorsement, all provisions of the Policy to which this endorsement is attached, as well as all terms and conditions, remain unchanged and applicable.

This endorsement extends certain coverages. The headers in this endorsement are only for convenience. Read the entire policy carefully to determine rights, duties and what is and is not covered.

In consideration of the premium charged for the Policy, it is hereby understood and agreed that:

I. The following Insuring Agreement is added to **SECTION I – INSURING AGREEMENTS:**

Service Fraud:

Subject to the Service Fraud Coverage Limit set forth above and any Deductible specified in the Declarations to this policy, We will pay for any monetary **Loss** sustained by **You**, including but not limited to phone and cloud based service bills, and Cryptojacking, first **Discovered** during the Policy Period and reported in accordance Condition **14. Duties in the Event of Claim or Loss** in **SECTION VI - CONDITIONS**, directly resulting from an intentional unauthorized access to Your **Telephone System** by a third party.

With respect to this Telecommunications Fraud Insuring Agreement:

a. **Loss** means the additional monetary costs incurred by **You** as a direct result of:

1. unauthorized calls or unauthorized use of **Your Telephone System's** bandwidth;
2. unauthorized access or use of **Your Cloud Based Services.***; and
3. unauthorized access or use of a **Computer System** for the purpose of mining for **Virtual Currency** with the use of any of the following services or resources:

- electricity
- natural gas
- oil
- internet.

b. Monetary Costs include only those additional amounts billed to **You** by the respective service provider, including usage or consumption information, incurred in a periodic billing statement pursuant to a written contract executed before the **Loss** first occurred with **You**, and does not

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

include any amounts charged at a flat fee that does not scale with the rate or use of the respective service due for payment during the **Policy Period**.

c. Telephone System means the Voice over Internet Protocol (VoIP) phone system directly under **Your** control.

d. Cloud Based Services means Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

e. Virtual Currency means a type of digital representation of currency or asset which is stored, transferred, and transacted in electronic form, utilizes cryptography to secure its network, regulate its generation, and verify its transfer, and operated independently of a central bank or other central authority in the majority of financial jurisdictions.*

II. The following is added to **SECTION II – LIMITS OF INSURANCE, 2. Aggregate Sublimit(s) of Insurance:**

The most We will pay for all Loss covered under the Service Fraud Insuring Agreement is the Service Fraud Aggregate Sublimit of Insurance, if any, shown above or in the Declarations., which are part of, and not in addition to, the Policy Aggregate Limit of Insurance. Upon exhaustion of any Aggregate Sublimit of Insurance by such payments, We will have no further obligations of liability of any kind with respect to **Loss** subject to such Sublimit of Insurance.

III. The following is added to **SECTION III – DEDUCTIBLE**

Under the Service Fraud Insuring Agreement, We will pay only the amount of **Loss** which is in excess of the Policy Deductible shown in the Declarations.

All other terms and conditions remain unchanged.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT

DEDICATED BREACH COSTS ENDORSEMENT

Security Breach Response Expense Coverage Limit:

This endorsement modifies insurance provided under the following:

COMMERCIAL CYBER INSURANCE POLICY

Unless modified by this Security Breach Response Expense Outside of Limit Endorsement, all provisions of the Policy to which this endorsement is attached, as well as all terms and conditions, remain unchanged and applicable.

This endorsement extends certain coverages. The headers in this endorsement are only for convenience. Read the entire policy carefully to determine rights, duties and what is and is not covered.

In consideration of the premium charged for the Policy, it is hereby understood and agreed that:

- I. Paragraph 1. **Policy Aggregate Limit of Insurance** of SECTION II – LIMITS OF INSURANCE is deleted in its entirety and replaced with the following:

1. Policy Aggregate Limit of Insurance

Except as provided below under Paragraph 3. **Security Breach Response Expense Limit of Insurance**, the most We will pay for all covered **Loss** and **Defense Expenses** is the Policy Aggregate Limit of Insurance shown in the Declarations. Furthermore, except as provided below under Paragraph 3. **Security Breach Response Expense Limit of Insurance**, the Policy Aggregate Limit of Insurance shall be reduced by any payment, including **Defense Expenses**, made under the terms of this Policy. Upon exhaustion of the Policy Aggregate Limit of Insurance and, only if applicable, the **Security Breach Response Expense Limit of Insurance**, We will have no further obligations or liability of any kind under this Policy.

- II. Paragraph 2. **Aggregate Sublimit(s) of Insurance** of SECTION II – LIMITS OF INSURANCE is deleted in its entirety and replaced with the following:

The Aggregate Sublimit(s) of Insurance set forth in the Declarations are part of, and not in addition to, the Policy Aggregate Limit of Insurance. Any such Aggregate Sublimit(s) of Insurance shall be reduced by any payment for **Loss** and, if applicable, **Defense Expenses**, under the Insuring Agreement to which such Aggregate Sublimit of Insurance applies. Upon exhaustion of any Aggregate Sublimit of Insurance by such payments, We will have no further obligations or liability of any kind with respect to **Loss** or **Defense Expenses**, subject to such Sublimit of Insurance.

2. Aggregate Sublimit(s) of Insurance

Except as provided below under Paragraph 3. **Additional Security Breach Response Expense Limit of Insurance**, Subject to the Policy Aggregate Limit of Insurance, the most We will pay for all Loss covered under:

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT

- a. Insuring Agreement 2 – Extortion Threats, is the Ransom Payments Aggregate Sublimit Of Insurance, if any, shown in the Declarations; and
- b. Insuring Agreement 4 – Business Income and Extra Expense (Security Failure and System Failure), is the Business Income and Extra Expense Aggregate Sublimit of Insurance, if any, shown in the Declarations.

The Aggregate Sublimit(s) of Insurance described in Paragraphs 2.a. and 2.b. above are part of, and not in addition to, the Policy Aggregate Limit of Insurance. Any such Aggregate Sublimit(s) of Insurance shall be reduced by any payment for **Loss** and, if applicable, **Defense Expenses**, under the Insuring Agreement to which such Aggregate Sublimit of Insurance applies. Upon exhaustion of any Aggregate Sublimit of Insurance by such payments, We will have no further obligations or liability of any kind with respect to **Loss** or **Defense Expenses**, subject to such Sublimit of Insurance.

III. The following is added to **SECTION II – LIMITS OF INSURANCE**:

3. Additional Security Breach Response Expense Limit of Insurance

Solely with respect to **SECTION I – INSURING AGREEMENTS, 1. Security Breach Response Expense**:

- a. All **Loss** covered under **SECTION I - INSURING AGREEMENTS, 1. Security Breach Response Expense** incurred by the **Named Insured** in excess of the Policy Deductible amount shown in the Declarations resulting directly from a **Security Breach** or **Cyber Incident Discovered** during the Policy Period or any extended reporting period, if applicable, shall only apply to, and reduce, the **Additional Security Breach Response Expense Limit of Insurance**. All such **Loss** shall not apply to or reduce the Policy Aggregate Limit of Insurance.
- b. Upon exhaustion of the **Additional Security Breach Response Expense Limit of Insurance** We will have no further obligations or liability of any kind **SECTION I – INSURING AGREEMENTS, 1. Security Breach Response Expense** under the Policy.

All other terms and conditions remain unchanged.

POLICYHOLDER DISCLOSURE

NOTICE OF TERRORISM INSURANCE COVERAGE

You are hereby notified that under the Terrorism Risk Insurance Act, as amended, you have a right to purchase insurance coverage for losses resulting from acts of terrorism, as defined, in Section 102(1) of the Act: The term "act of terrorism" means any act or acts that are certified by the Secretary of the Treasury—in consultation with the Secretary of Homeland Security, and the Attorney General of the United States—to be an act of terrorism; to be a violent act or an act that is dangerous to human life, property, or infrastructure; to have resulted in damage within the United States, or outside the United States in the case of certain air carriers or vessels or the premises of a United States mission; and to have been committed by an individual or individuals as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion. Where coverage is provided under this Policy, any losses resulting from certified acts of terrorism may be partially reimbursed by the United States Government under a formula established by the Terrorism Risk Insurance Act, as amended. However, your policy may contain other exclusions which might affect your coverage, such as an exclusion for nuclear events. Under the formula, the United States Government generally reimburses 80% beginning on January 1, 2020, of covered terrorism losses exceeding the statutorily established deductible paid by the insurance company providing the coverage. The Terrorism Risk Insurance Act, as amended, contains a \$100 billion cap that limits U.S. Government reimbursement as well as insurers' liability for losses resulting from certified acts of terrorism when the amount of such losses exceeds \$100 billion in any one calendar year. If the aggregate insured losses for all insurers exceed \$100 billion, your coverage may be reduced.

Your premium will include the additional premium for terrorism, as stated in the section of this Notice titled DISCLOSURE OF PREMIUM.

DISCLOSURE OF PREMIUM

Your premium for terrorism coverage is: \$0 (This charge/amount is applied to obtain the final premium).

You may choose to reject the offer by selecting the rejection option below. If you choose to reject the offer, Your Policy will be modified to exclude the described coverage. If you choose to accept this offer, you do not need to do anything further and such coverage will be provided as described herein.

REJECTION OF TERRORISM INSURANCE COVERAGE

- By clicking this box, I affirm that I have read this Notice and hereby choose to decline to purchase coverage for certified acts of terrorism, as defined in Section 102(1) of the Act. I understand that I will not have coverage for any losses resulting from any certified acts of terrorism and that an exclusion of certain terrorism losses will be made part of this Policy.

Policyholder/Applicant's Signature

Named Insured

Print Name of Policyholder/Applicant

Spinnaker Insurance Company
Insurance Company

Date:

Policy Number:

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

FUNDS TRANSFER FRAUD AND SOCIAL ENGINEERING COVERAGE

Funds Transfer Fraud Coverage Limit:
Social Engineering Fraud Coverage Limit:
Funds Transfer Fraud Deductible:
Social Engineering Fraud Deductible:

This endorsement modifies insurance provided under the following:

COMMERCIAL CYBER INSURANCE POLICY

With regard to this Funds Transfer Fraud and Social Engineering endorsement, the provisions of the Policy to which this endorsement is attached remain unchanged and apply, unless modified by this endorsement.

In consideration of the premium charged for the Policy, it is hereby understood and agreed that:

I. The following Insuring Agreement is added to **SECTION I – INSURING AGREEMENTS:**

Funds Transfer Fraud

a. Subject to the Funds Transfer Fraud Coverage Limit and Deductible set forth above, We will pay for:

i. **Loss** resulting directly from a fraudulent:

1. Entry of **Electronic Data or Computer Program** into; or
2. Change of **Electronic Data or Computer Program** within;

a **Computer System**, by a person or organization without authorization to access such **Computer System**; or

ii. **Loss** resulting directly from a **Fraudulent Instruction** directing a financial institution to debit Your **Transfer Account** and transfer, pay or deliver **Money** or **Securities** from that account without Your knowledge or consent;

that is first **Discovered** during the Policy Period or any Extended Reporting Period, if applicable, and reported in accordance with Condition **14. Duties in the Event of Claim or Loss** in **SECTION VI – CONDITIONS.**

II. The following Insuring Agreement is added to **SECTION I – INSURING AGREEMENTS:**

Social Engineering

a. Subject to the Social Engineering Coverage Limit and Deductible set forth above, We will pay for **Social Engineering Loss** resulting directly from a **Social Engineering Incident** involving an **Insured's** loss of **Money**, that is first **Discovered** during the Policy Period or any Extended Reporting Period, if applicable, and reported in accordance with Condition **14. Duties in the Event of Claim or Loss** in **SECTION VI – CONDITIONS.**

III. Solely with respect to the coverage afforded under this endorsement:

a. **Computer Program** means a set of related electronic instructions, which direct the operation and function of a computer or devices connected to it, which enables the computer or devices to receive, process, store or send Your **Electronic Data**.

b. **Loss** means:

1. In Paragraph I.a.i.:

- a. Your **Money, Securities** or other property fraudulently transferred, paid or delivered; or
- b. **Money** or **Securities** fraudulently debited or deleted from Your account at a financial institution.

2. In Paragraph I.a.ii., **Money** or **Securities** transferred, paid, or delivered from Your **Transfer Account**.

c. **Fraudulent Instruction** means:

i. With regard to Paragraph I.a.ii.:

- a. A computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic instruction, including instructions produced or manipulated by deep fakes, synthetic media, or other artificial intelligence technologies, directing a financial institution to debit Your **Transfer Account** and to transfer, pay or deliver **Money** or **Securities** from that **Transfer Account**, which instruction purports to have been issued by You, but which in fact was fraudulently issued by someone else without Your knowledge or consent.
- b. A written instruction issued to a financial institution directing the financial institution to debit Your **Transfer Account** and to transfer, pay or deliver **Money** or **Securities** from that **Transfer Account** through an electronic funds transfer system at specified times or under specified conditions, which instruction purports to have been issued by You, but which in fact was issued, forged or altered by someone else without Your knowledge or consent.

ii. With regard to a **Social Engineering Incident**:

A computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic or voice instruction, including instructions produced or manipulated by deep fakes, synthetic media, or other artificial intelligence technologies, received and relied upon by the **Insured** that causes the transfer, payment or delivery of Your **Money**, which instruction purports to have been issued by You or Your **Vendor**, but which in fact was fraudulently issued by someone else.

d. **Transfer Account** means an account maintained by You at a financial institution from which You can initiate the transfer, payment or delivery of **Money** and **Securities**:

- 1. By means of computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic instructions; or
- 2. By means of written instructions establishing the conditions under which such transfers are to be initiated by such financial institution through an electronic funds transfer system.

e. **Money** means currency, coins or bank notes in current use and having a face value, travelers' checks, register checks and money orders held for sale to the public. The term **Money** does not include digital currency or other negotiable and nonnegotiable instruments or contracts representing either **Money** or property.

f. **Securities** mean negotiable and non-negotiable instruments or contracts representing either Money or property.

Securities does not include **Money**.

g. Social Engineering Incident means the intentional misleading of an **Insured** to transfer **Money** to a person, place or account beyond the **Named Insured's** control resulting directly from the **Named Insured's** employee's good faith reliance upon an instruction transmitted electronically, purporting to be from:

1. a **Vendor**;
2. an employee of the **Named Insured**;

but which contained a **Fraudulent Instruction** or material misrepresentation and was sent by an imposter.

h. Social Engineering Loss means the loss of **Money** as a result of a **Social Engineering Incident**.

Social Engineering Loss does not include indirect and/or consequential loss.

i. Vendor means:

1. a natural person or entity who exchanges, or is under contract to exchange, goods or services with the **Named Insured** for a fee (other than a financial institution, asset manager, broker-dealer, armored motor vehicle "named insured" or any similar entity); or
2. a computer software contractor who has a written agreement with the **Named Insured** to design, implement or service **Computer Programs** for a covered **Computer System**;

provided such person, entity or contractor is not owned, operated, or controlled by the **Named Insured**.

IV. The following is added to **SECTION II – LIMITS OF INSURANCE, 2. Aggregate Sublimit(s) of Insurance**:

- a.** The most We will pay for all Loss covered under the Funds Transfer Fraud Insuring Agreement is the Funds Transfer Fraud Sublimit of Insurance shown above, which is part of, not in addition to the Policy Aggregate Limit of Insurance set forth in the Declarations to this Policy. Upon exhaustion of any Aggregate Sublimit of Insurance by such payments, We will have no further obligations or liability of any kind with respect to **Loss** subject to such Sublimit of Insurance.
- b.** The most We will pay for all Loss covered under the Social Engineering Insuring Agreement is the Social Engineering Sublimit of Insurance shown above, which is part of, not in addition to the Policy Aggregate Limit of Insurance set forth in the Declarations to this Policy. Upon exhaustion of any Aggregate Sublimit of Insurance by such payments, We will have no further obligations or liability of any kind with respect to **Loss** subject to such Sublimit of Insurance.

V. The following is added to **SECTION III – DEDUCTIBLE**:

Under the Funds Transfer Fraud Insuring Agreement, We will pay only the amount of **Loss** which is in excess of the Policy Deductible shown above, or shown in the Declarations.

Under the Social Engineering Insuring Agreement, We will pay only the amount of **Loss** which is in excess of the Policy Deductible shown above, or in the Declarations.

VI. The following is added to **SECTION V – EXCLUSIONS**:

a. Solely with respect to coverage provided under the Funds Transfer Fraud Insuring Agreement, We will not be liable for **Loss** based upon, attributable to, arising out of or resulting from:

i. A fraudulent:

1. Entry of **Electronic Data** or **Computer Program** into; or

2. Change of **Electronic Data** or **Computer Program** within

a **Computer System**, by a person or organization with authorized access to such **Computer System**.

- ii. The use or purported use of credit, debit, charge, access, convenience, identification, stored-value or other cards or the information contained on such cards.
- iii. The giving or surrendering of property in any exchange or purchase.
- iv. A financial institution acting upon any instruction to:
 - 1. Transfer, pay or deliver **Money, Securities** or other property; or
 - 2. Debit or delete Your account;

which instruction proves to be a fraudulent, dishonest or criminal act by any **Employee** or authorized representative of the **Named Insured**, whether acting alone or in collusion with others.

- b. Solely with respect to coverage provided under the Funds Transfer Fraud Insuring Agreement, We will not be liable for **Loss**, or that part of any **Loss**, the proof of which as to its existence or amount is dependent upon:
 - i. An inventory computation; or
 - ii. A profit and loss computation.
- c. Solely with respect to coverage provided under the Social Engineering Insuring Agreement, We will not be liable for **Social Engineering Loss** resulting from a **Social Engineering Incident** based upon, attributable to, arising out of or resulting from:
 - i. An actual or alleged infringement of, violation of, misappropriation of or assertion of any right to or interest in any:
 - 1. Patent, copyright, trademark, trade dress, certification mark, collective mark, service mark, expression, idea, likeness, name, slogan, style of doing business, symbol, title, trade secret or other intellectual property right by or on behalf of any **Insured**; or
 - 2. Software or computer code or its source content or material by or on behalf of any **Insured**.
 - ii. A fraudulent, dishonest or criminal act by any **Employee** or authorized representative of the **Named Insured**, whether acting alone or in collusion with others.
 - iii. The establishment of any credit or similar promise to pay, or to any party's use of or acceptance of any credit card, debit card or similar instrument, whether or not genuine.
 - iv. Any investment or ownership in any corporation, partnership, real property, or similar instrument, whether or not such investment is genuine.
 - v. A kidnap, ransom or other extortion payment surrendered as a result of a threat to do bodily harm to any natural person or a threat to harm, take, or transfer property.

VII. **SECTION VI – CONDITIONS**, Condition 14. **Duties in the Event of Claim or Loss** is amended to include reference and be applicable to the Funds Transfer Fraud Insuring Agreement and the Social Engineering Insuring Agreement.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

CONTINGENT BUSINESS INCOME – SYSTEM FAILURE (IT)

This endorsement modifies insurance provided under the following:

COMMERCIAL CYBER INSURANCE POLICY

Unless modified by this Contingent Business Income - System Failure (IT) Endorsement, all provisions of the Policy to which this endorsement is attached, as well as all terms and conditions, remain unchanged and applicable.

In consideration of the premium charged for the Policy, it is hereby understood and agreed that:

I. The following Insuring Agreement is added to **SECTION I – INSURING AGREEMENTS**:

Contingent Business Income – System Failure (IT)

Subject to the Business Income and Extra Expense (Security Failure and System Failure) Coverage Limit and any Deductible specified in the Declarations to this policy, We will pay for **Loss** incurred during an **Interruption** resulting directly from a **System Failure** of a **Computer System** operated by a **Third Party** that is **Discovered** during the Policy Period or during any Extended Reporting Period, if applicable and reported in accordance with Condition **14. Duties in the Event of Claim or Loss in SECTION VI – CONDITIONS**.

With respect to this Contingent Business Income – System Failure (IT) Insuring Agreement:

- a. **Loss** means the actual **Loss** of (1) “contingent business income” You sustain and/or (2) “extra expense” You incur as a result of a **System Failure** of a **Computer System** operated by a **Third Party** which:
- i. collects, transmits, processes, stores or retrieves Your **Electronic Data**; or
 - ii. is owned or leased by a **Third Party**.

Loss does not include:

- (1) Loss arising out of any liability to any third party;
- (2) Legal costs or expenses.

- b. “Contingent business income” means the:

- i. net income (net profit or loss before income taxes) that would have been earned or incurred; and
- ii. continuing normal operating expenses incurred, including payroll.

“Contingent business income” does not include:

- (1) Continuing normal operating expenses incurred, including payroll, if there has been no net income (net profit or loss before income taxes) that would have been earned or incurred as set forth in paragraph a.i. above; and/or

- (2) Net Profit that would likely have been earned as a result of an increase in volume due to favorable business conditions caused by the impact of network security failures impacting other businesses, loss of market, or any other consequential loss.

c. "Extra expense" means necessary and reasonable expenses You incur:

- i. during an **Interruption** that You would not have incurred if there had been no **Interruption**; and
- ii. during an **Interruption** in order to minimize or reduce loss of "Contingent Business income".

"Extra expense" does not include:

- (1) any costs or expenses associated with upgrading, maintaining, repairing, remediating or improving a **Computer System** as a result of a **Cyber Incident, Extortion Threat, or System Failure**; or
- (2) **Extortion Expenses** covered under Insuring Agreement 2 – Extortion Threats.

II. The following is added to **SECTION VII – DEFINITIONS**:

1. **Interruption** means:

c. With respect to a **System Failure**:

- i. an unanticipated cessation or slowdown of Your business operations; or
- ii. Your voluntary suspension of Your business operations;

resulting directly from a **System Failure** of a **Computer System** operated by a **Third Party**;

and, with regard to Paragraphs i and ii. above, shall be deemed to begin when Your business operations are interrupted and ends at the earliest of:

- (1) one hundred-eighty (180) days after the **Interruption** begins;
- (2) the time when Your business operations are resumed; or
- (3) the time when service is restored to You.

2. **System Failure** means any sudden, unintentional, or unexpected and continuous outage, degradation or failure of a **Computer System** which disrupts, prevents, or restricts the normal functioning of Your business operations which would otherwise have been handled in whole or in part by the **Computer System** and is directly caused by a malfunction in normal computer function or network service, or hardware failure.

System Failure does not include:

- (1) failure of hardware or software due to product defects or design/manufacturing flaws, ordinary wear and tear of physical components, or use of hardware past End of Life Announcements (EOLA) or Last Date of Support (LODS);
- (2) failure of a **Computer System** operated by a **Third Party** which results in an extended outage beyond the services performed for you by the **Third Party**;
- (3) failure to adequately anticipate or capacity plan for expected and/or above-normal

operational demand for a **Computer Systems**, however, this exclusion shall not apply if such operational demand is caused by a denial of service attack;

- (4) failure to renew any domain names or uniform resource locators;
- (5) failure of a **Computer System** caused by a **Cyber Incident**; or
- (6) voluntary suspension or shutdown of a **Computer System** operated **Third Party**.

III. Condition 16. **Valuation – Settlement** in **SECTION VI – CONDITIONS** is deleted in its entirety and replaced with the following:

Valuation – Settlement

All premiums, limit(s) of insurance, deductible amounts, **Loss** and any other monetary amounts under this Policy are expressed and payable in the currency of the United States of America. If judgment is rendered, settlement is agreed to or another component of **Loss** under this Policy is expressed in any currency other than United States of America dollars, payment under this Policy shall be made in United States dollars at the rate of exchange published in The Wall Street Journal on the date the final judgment is entered, settlement amount is agreed upon or the other component of **Loss** is due, respectively.

- a. With respect to **Loss** covered under the Business Income and Extra Expense (Security Failure and System Failure) and the Contingent Business Income – Security Failure Insuring Agreements, the amount of “business income” and “contingent business income” will be determined based on consideration of:
 - i. the net income generated from Your business operations before the **Interruption** occurred;
 - ii. the likely net income generated by Your business operations if no **Interruption** had occurred, but not including any net income that would likely have been earned as a result of an increase in the volume of business due to favorable business conditions caused by the impact of the **Cyber Incident** on customers or on other businesses;
 - iii. the operating expenses, including payroll, necessary to resume Your business operations with the same quality of service that existed before the **Interruption**; and
 - iv. other relevant sources of information, including Your financial records and accounting procedures, bills, invoices and other vouchers, and debts, liens and contracts.

However, the amount of “business income” and “contingent business income” will be reduced to the extent that the reduction in the volume of business from the affected business operations is offset by an increase in the volume of business from other channels of commerce such as via telephone, mail or other sources.

- b. With respect to **Loss** covered under the Business Income and Extra Expense (Security Failure and System Failure) and the Contingent Business Income – Security Failure (IT) Insuring Agreements, the amount of “business income” and “contingent business income”, the amount of “extra expense” will be determined based on:
 - i. necessary expenses that exceed the normal operating expenses that would have been incurred in the course of Your business operations during the period of coverage if no **Interruption** had occurred. We will deduct from the total of such expenses the salvage value that remains of any property bought for temporary use during the period of coverage once Your business operations are resumed; and

- ii. necessary expenses that reduce the "business income" and "contingent business income" **Loss** that otherwise would have been incurred during the period of coverage.

All other terms and conditions remain unchanged.

SPECIMEN

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

CONTINGENT BUSINESS INCOME – SECURITY FAILURE

This endorsement modifies insurance provided under the following:

COMMERCIAL CYBER INSURANCE POLICY

Unless modified by this Contingent Business Income – Security Failure Endorsement, all provisions of the Policy to which this endorsement is attached, as well as all terms and conditions, remain unchanged and applicable.

In consideration of the premium charged for the Policy, it is hereby understood and agreed that:

I. The following Insuring Agreement is added to **SECTION I – INSURING AGREEMENTS**:

Contingent Business Income – Security Failure

Subject to the Business Income and Extra Expense Aggregate Sublimit and any Deductible specified in the Declarations to this policy, We will pay for **Loss** incurred during an **Interruption** resulting directly from a **Cyber Incident** or **Extortion Threat** of a **Computer System** operated by a **Third Party** that is **Discovered** during the Policy Period or during any Extended Reporting Period, if applicable and reported in accordance with Condition **14. Duties in the Event of Claim or Loss in SECTION VI – CONDITIONS**.

With respect to this Contingent Business Income – Security Failure Insuring Agreement:

a. **Loss** means the actual **Loss** of (1) “contingent business income” You sustain and/or (2) “extra expense” You incur as a result of a **Cyber Incident** or **Extortion Threat** of a **Computer System** operated by a **Third Party** which:

- i. collects, transmits, processes, stores or retrieves Your **Electronic Data**; or
- ii. is owned or leased by a **Third Party**.

Loss does not include:

- (1) Loss arising out of any liability to any third party; or
- (2) Legal costs or expenses.

b. “Contingent business income” means the:

- i. measurable net income (net profit or loss before income taxes) that would have been earned or incurred; and
- ii. continuing normal operating expenses incurred, including payroll.

“Contingent business income” does not include:

- (1) Continuing normal operating expenses incurred, including payroll, if there has been no net income (net profit or loss before income taxes) that would have been earned or incurred as set forth in paragraph a.i. above; and/or

- (2) Net Profit that would likely have been earned as a result of an increase in volume due to favorable business conditions caused by the impact of network security failures impacting other businesses, loss of market, or any other consequential loss.

c. "Extra expense" means necessary and reasonable expenses You incur:

- i. in excess of Your normal operating expense during an **Interruption** that You would not have incurred had no **Interruption** occurred; and
- ii. during an **Interruption** in order to minimize or reduce loss of "Contingent Business income".

"Extra expense" does not include:

- (1) any costs or expenses associated with upgrading, maintaining, repairing, remediating or improving a **Computer System** as a result of a **Cyber Incident** or **Extortion Threat**; or
- (2) **Extortion Expenses** covered under Insuring Agreement 2 – Extortion Threats.

II. The **Interruption** definition in **SECTION VII – DEFINITIONS** is deleted in its entirety and replaced with the following:

Interruption means:

a. With respect to a **Cyber Incident** or **System Failure**:

- i. an unanticipated cessation or slowdown for Your business activities; or
- ii. Your voluntary suspension of Your business operations for the purpose of avoiding or mitigating the possibility of transmitting a **Virus** or malicious code to another person or organization;

and, with regard to Paragraphs a.i and a.ii. above, shall be deemed to begin when Your business operations are interrupted and ends at the earliest of:

- (1) one hundred-eighty (180) days after the **Interruption** begins;
- (2) the time when Your business operations are resumed; or
- (3) the time when service is restored to You.

b. With respect to an **Extortion Threat**, Your voluntary suspension of Your business operations:

- i. based upon clear evidence of a credible threat; or
- ii. based upon the recommendation of a security firm, if any;

and, with regard to Paragraphs b.i and b.ii. above, shall be deemed to begin when Your business operations are interrupted and ends at the earliest of:

- (1) one hundred-eighty (180) days after the **Interruption** begins;
- (2) the time when Your business operations are resumed; or
- (3) the time when service is restored to You.

III. Condition 16. **Valuation – Settlement** in **SECTION VI – CONDITIONS** is deleted in its entirety and replaced with the following:

16. **Valuation – Settlement**

All premiums, limit(s) of insurance, deductible amounts, **Loss** and any other monetary amounts under this Policy are expressed and payable in the currency of the United States of America. If judgment is rendered, settlement is agreed to or another component of **Loss** under this Policy is expressed in any currency other than United States of America dollars, payment under this Policy shall be made in United States dollars at the rate of exchange published in The Wall Street Journal on the date the final judgment is entered, settlement amount is agreed upon or the other component of **Loss** is due, respectively.

- a. With respect to **Loss** covered under the Business Income and Extra Expense Insuring Agreements, the amount of “business income” and “contingent business income” will be determined based on consideration of:
- i. the net income generated from Your business activities before the **Interruption** occurred;
 - ii. the likely net income generated by Your business activities if no **Interruption** had occurred, but not including any net income that would likely have been earned as a result of an increase in the volume of business due to favorable business conditions caused by the impact of the **Cyber Incident** on customers or on other businesses;
 - iii. the operating expenses, including payroll, necessary to resume Your business activities with the same quality of service that existed before the **Interruption**; and
 - iv. other relevant sources of information, including Your financial records and accounting procedures, bills, invoices and other vouchers, and debts, liens and contracts.

However, the amount of “business income” and “contingent business income” will be reduced to the extent that the reduction in the volume of business from the affected business activities is offset by an increase in the volume of business from other channels of commerce such as via telephone, mail or other sources.

- b. With respect to **Loss** covered under the Business Income and Extra Expense and the Contingent Business Income – Security Failure Insuring Agreements, the amount of “business income” and “contingent business income”, the amount of “extra expense” will be determined based on:
- i. necessary expenses that exceed the normal operating expenses that would have been incurred in the course of Your business activities during the period of coverage if no **Interruption** had occurred. We will deduct from the total of such expenses the salvage value that remains of any property bought for temporary use during the period of coverage once Your business activities are resumed; and
 - ii. necessary expenses that reduce the “business income” and “contingent business income” **Loss** that otherwise would have been incurred during the **Interruption**.

All other terms and conditions remain unchanged.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

BLANKET ADDITIONAL INSURED ENDORSEMENT

This endorsement modifies insurance provided under the following:

COMMERCIAL CYBER INSURANCE POLICY

Unless modified by this Endorsement, all provisions of the Policy to which this endorsement is attached, as well as all terms and conditions, remain unchanged and applicable.

In consideration of the premium charged for the Policy, it is hereby understood and agreed that:

I. The following additional provision is added to **SECTION I – INSURING AGREEMENTS, 6. Security Breach Liability** Including Payment Card Industry (PCI) Fines and Penalties:

e. **Loss and Defense Expenses**, on behalf of an **Additional Insured**, as a result of a **Claim** that is **Discovered** during the Policy Period and reported to Us during the **Policy Period** of any **Extended Reporting Period**, if applicable, resulting from a **Wrongful Act** or a series of **Interrelated Wrongful Acts**, taking place on or after Your first date of continuous coverage with Us and before the end of the **Policy Period**.

However, this coverage shall only apply if:

- i. Prior to such **Claim** being made against the **Additional Insured**, the **Named Insured** entered into a written contract or agreement with the **Additional Insured** that requires the **Named Insured** to indemnify such **Additional Insured**;
- ii. Such coverage is limited to **Loss and Defense Expenses** which, had the **Claim** been made against the **Named Insured**, would have been covered under this Policy; and
- iii. Such claim against the **Additional Insured** is solely as a result of any actual or alleged **Wrongful Act** by, or asserted against, the **Additional Insured**.

II. Solely with respect to the coverage provided under this endorsement, the following definition is added **SECTION VII – DEFINITIONS**:

Additional Insured means any person or organization which the **Named Insured** is required, under written contract or agreement executed prior to the **Wrongful Act**, to include as an **Additional Insured** for the type of coverage afforded under this Policy.

All other terms and conditions remain unchanged.

POLICY DOCUMENTATION DELIVERY METHOD SELECTION FORM

Spinnaker Insurance Company is required by law to obtain Your consent to engage in electronic delivery of Your policy and related forms. You may:

- Select ONLY electronic delivery;
- Select ONLY paper delivery;
- Select BOTH electronic delivery and paper delivery; or
- Withdraw Your previous consent to receive electronic delivery.

Please indicate Your choice from the options below. Your selection applies to You and any other insureds entitled to receive copies of such forms under the policy.

ELECTRONIC DELIVERY ONLY

I select electronic delivery of the form(s) indicated below. I acknowledge that I will not receive paper copies of these form(s), unless I notify Spinnaker Insurance Company or my agent/broker of my decision to entirely withdraw electronic consent or modify my selection to also include paper delivery.

- Policy
- Notices of Cancellation and Nonrenewal
- Other forms related to my policy

PAPER DELIVERY ONLY

I select paper delivery of my policy and all related forms. I acknowledge that I will only receive paper copies of such forms.

BOTH ELECTRONIC DELIVERY AND PAPER DELIVERY

I select the option to receive both electronic and paper delivery of my policy and all related forms.

WITHDRAWAL OF CONSENT OF ELECTRONIC DELIVERY

I withdraw my consent to receive electronic delivery of my policy and/or related forms. In the future, I will only receive paper copies of such forms.

DISCLOSURE

If You elect to have Your insurance policy and related documents sent to You by electronic delivery, it is Your responsibility to update Your email address should it change at any time during the life of the policy. Further, Your election to have Your insurance policy and related documents transmitted to You electronically shall remain in effect until You notify:

Spinnaker Insurance Company
c/o Boost Insurance Agency, Inc.
22 W 21st Street, 7th Floor
New York, NY 10010

in writing of Your withdrawal of such consent.

Name of Individual to Receive Documents by Electronic Delivery

E-mail Address of Individual to Receive Documents by Electronic Delivery

First Named Insured

Print Name of First Named Insured's Authorized Representative

Signature of First Named Insured's Authorized Representative

Date

SPECIMEN

Spinnaker Privacy Policy

Last Updated: August 2024

This privacy policy applies to Spinnaker Insurance Company and its wholly-owned subsidiaries (collectively, “**Spinnaker**,” “**we**,” “**our**” and “**us**”). This privacy policy applies to information collected offline and information obtained from third parties (collectively “**Services**”).

This privacy policy describes the information we collect about you, how we use this information and the choices you have regarding such use, and other important information regarding our privacy practices. If you have any questions or comments about this privacy policy or the ways in which Spinnaker uses the information we collect about you, please contact us using the information provided in the contact section below.

Please note the Spinnaker Consumer Privacy Notice applies to information that we collect about individuals who seek, apply for, or obtain our insurance products or services for personal, family or household purposes, whether that information comes through our Services or any other means. The information contained in this privacy policy is not intended to amend, replace, contradict, change, or otherwise affect the policies outlined in the Spinnaker Consumer Privacy Notice. Please read the Spinnaker Consumer Privacy Notice for information about your rights with respect to the information collected in connection with seeking, applying for, or obtaining insurance products or services from us. If you are a California consumer, you may find the California Financial Information Privacy Act Notice after our Consumer Privacy Notice.

Before engaging with us, submitting information to us, or buying or using our Services, please review this privacy policy carefully.

You may print or download a pdf version of this privacy policy.

Table of Contents

1. We may collect your information when you use our Services, when you apply for products, or from third parties.
2. We may collect information you provide us when you use our Services.
3. We may collect your information when you apply for or use our Services.
4. We may collect your personal information from third parties.
5. We may use your information to provide you with our Services.
6. We may retain your information for our business purposes.
7. We may share your information to provide you with our Services.
8. You can manage your browser cookies.
9. We do not respond to Do Not Track signals.
10. We may provide links to other companies.
11. We may record calls to our call centers and in-house agents.
12. We encourage caution in posting information publicly.
13. We take measures to protect your personal information.
14. Our Services are not intended for minors.
15. We provide you with additional disclosures relating to various state privacy laws.
16. You may have additional rights under various state privacy laws.

17. Victims of domestic violence may have confidentiality rights.
18. We are based in the United States.
19. We may change this privacy policy.
20. Spinnaker provides you with a Consumer Privacy Notice.
21. Spinnaker provides you with a California Financial Information Privacy Act Notice.
22. You may contact us.

1. We may collect your information when you use our Services, when you apply for products, or from third parties.

We may collect information from you in various ways, including the following:

- We collect information you provide us when you use our Services;
- We collect information when you apply for or use our Services; and
- We collect information from third parties, such as our service providers, data providers, or partners.

2. We may collect information you provide us when you use our Services.

When you use our Services, we may collect the information you provide us, for example, when you:

- Ask a question;
- Email us or modify your account;
- Conduct transactions;
- Apply for Services;
- Begin or complete a form;
- Modify your coverage;
- Inquire about the status of a claim;
- Contact customer support; and
- Provide feedback or a complaint.

3. We may collect your information when you apply for or use our Services.

We may collect information when you apply for or use our Services, including:

- Name, email address, postal address, or residential property address;
- Driver's license number;
- Date of birth;

NOT BINDING

- Your signature, phone number, and family member information;
- Payment card information, financial account information, or insurance policy information;
- Age, gender, marital status, and veteran or military status;
- Payment history, claims history, property information and records;
- Records of Services requested or purchased;
- Lender information, and information necessary to determine discount qualification and eligibility; and
- Other information you provide to us.

Some forms on our Services may require that you provide certain information to submit the form. You may choose not to provide information in those cases, but this may prevent you from being able to use certain features of our Services.

4. We may collect your personal information from third parties.

We may collect personal information about you from third parties. In some instances, we may combine the personal information we collect about you from third parties with personal information we collect from you. We also may obtain personal information about you from consumer reporting agencies or insurance support organizations as well as from commercially available sources such as data aggregators and public databases. Depending on your relationship with us, this personal information we collect from third parties may include:

- Name, email address, postal address, or residential property address;
- Information about your property, including its condition; or
- Demographic information.

Additionally, if you purchase insurance through an insurance agent or agency, we may receive personal information from the agent or agency about you, including information listed in Section 3. We may also receive information about you from public databases or third parties from whom we have obtained data, among other sources. We may combine this information with other information we have about you.

5. We may use your information to provide you with our Services.

We may use your information in a variety of ways, including to:

- Complete an application on your behalf;
- Communicate insurance information to a lender or mortgagor designated by you;
- Service your policy;
- Intake and process claims;
- Respond to your requests, questions, or comments;
- Send billing notices to you and your lender, mortgagor, or lender service company;
- Communicate with you and others;
- Develop new Services;

- Improve our existing Services;
- Address problems and review the usage and operations of our Services or business;
- Improve our Services, content, products, and offerings;
- Protect the security and integrity of our Services and our business, including to detect fraud or illegal activities;
- Enforce our terms of use and other applicable policies;
- Conduct actuarial or research studies;
- Protect and defend our rights and property or the rights of third parties; and
- As otherwise described to you at the point of collection.

6. We may retain your information for our business purposes.

We may retain and use your information in accordance with our records retention schedule, as required or permitted by law, to comply with our legal obligations, to resolve disputes, and to enforce our agreements. We also retain your information as needed to provide Services to you and while you maintain an account with us.

7. We may share your information to provide you with our Services.

In addition to sharing your information as described at time of collection, we may share your information with the following persons or entities or in the following circumstances, among others:

- When we have your consent or at your direction;
- To perform or provide the Services you requested;
- With a parent, subsidiary, or affiliate entity within the Spinnaker corporate family, as permitted by law;
- With third parties that play a role in an insurance or other transaction such as insurance companies, payment vendors, inspection companies, loss control companies, claims adjusters and other claims-related companies, contractors, investigators, attorneys and other third parties who provide services relating to your claim or a service that we offer;
- With participating insurance support organizations (information obtained from a report prepared by an insurance-support organization may be retained by the insurance-support organization and disclosed to other persons), reinsurance companies, and regulators;
- With our authorized agents and brokers who sell or facilitate the sale of our Services;
- With our vendors, as needed to perform their functions for us;
- With third parties to provide you with a product or service, as permitted by law;
- With legal entities, if required by law, or a regulatory authority or at the request of governmental, law enforcement, or regulatory authorities;
- When we believe such sharing is necessary, such as to protect the rights, property, life, security, or safety of Spinnaker or others; and
- In the case of a corporate transaction, such as a merger, acquisition, or divestiture.

8. You can manage your browser cookies.

Most internet browsers allow you to block, manage, or delete cookies or local storage through the privacy features of your browser. Please refer to the help section of your browser or mobile device for additional information. Your browser may also offer add-ons, plugins, or extensions to manage local storage objects, scripts, or similar technologies mentioned in our privacy policy. Please note that if you block cookies or similar technologies, you may not be able to use the full functionality of our Services. For further information about cookies and similar technologies, including how to manage and delete cookies on your device, you can visit [All About Cookies](#).

9. We do not respond to Do Not Track signals.

Our Services do not currently respond to Do Not Track signals. To learn more about Do Not Track signals, you may visit [the Future of Privacy Forum's website](#) for additional information.

10. We may provide links to other companies.

Our Services, other materials, and products may contain references or links to third-party websites and services, including references and links to third parties that accept and process your payments to us. We are not responsible for any third party's data collection or privacy practices, and we have no control over what information third parties track or collect. Any access to and use of such linked websites is not governed by this privacy policy but instead is governed by the privacy policies of those third-party websites. We encourage you to review the privacy policies posted on those third-party websites for further information.

11. We may record calls to our call centers and in-house agents.

We may record or monitor our conversations with you if you call our customer service centers or if our customer service centers or agents call you. We may use these recordings for business records, training, quality assurance, fraud prevention, and other business purposes. We may use your voiceprint for verification or anti-fraud purposes when you call our call centers or in-house agents.

12. We encourage caution in posting information publicly.

Our Services may permit you to post or submit content publicly. If you choose to submit content containing personal information to any public area of our Services, your content will be accessible by anyone, including us. We encourage you to exercise caution when making decisions about what you disclose publicly.

13. We take measures to protect your personal information.

We may take reasonable measures designed to secure your personal information. However, we cannot guarantee that your personal information will not be lost, accessed without authorization, disclosed, altered, or destroyed. Any information you provide to us is at your own risk.

14. Our Services are not intended for minors.

Our Services are not intended for children under the age of 13. We do not knowingly collect any personal information from anyone under the age of 13. You must be 18 years of age or older to submit any information to us.

15. We provide you with additional disclosures relating to various state privacy laws.

You may have additional privacy rights that we describe in further detail below.

Various state comprehensive privacy laws give individuals the right to know what personal information is collected about them, including whether it is being sold or disclosed to third parties. These state privacy laws also grant these individuals certain rights and prevent companies from retaliating against consumers for exercising those rights. This notice applies to all activities of Spinnaker, including those activities that occur online and offline.

The types of personal information we have collected or disclosed in the last twelve (12) months or beyond depend on your relationship with Spinnaker. If the nature of your relationship with Spinnaker changes, an additional data privacy notice may apply.

The personal information that Spinnaker collects about you may include the following categories of personal information:

1. Identifiers, such as real name, alias, postal address, unique personal identifier, online identifier, email address, account name, driver's license number, passport number, or other similar identifiers;
2. Personal information described in California Civil Code Section 1798.80(e), such as signature, physical characteristics or description, telephone number, insurance policy number, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information;
3. Characteristics of protected classifications under California or federal law, such as race, gender, physical or mental disability, and religion;
4. Commercial information, such as records of personal property, Services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
5. Biometric information, such as your voiceprint when you call our call centers;
6. Internet or other electronic network activity information, such as browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;
7. Geolocation data, such as information used to identify your physical location, including geolocation data collected in connection with your use of our Services;
8. Audio, electronic, visual, thermal, olfactory, or similar information;
9. Professional or employment-related information, such as information collected from job applications and resumes;
10. Education information, such as information collected from job applications, transcripts, or resumes;
11. Inferences, such as those drawn from any of the information Spinnaker collects to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes; and
12. Sensitive personal information, such as driver's license number, passport number, account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account, precise geolocation, racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or immigration status.

Types of Personal Information	Do we collect it?	Categories of Sources	Purposes of Collection	Do we disclose it to third parties?	Purposes of Disclosure	Categories of Third Parties PI Disclosed To	Do we sell it to third parties?	Purposes of Selling	Do we Share for Behavioral Advertising?	Retention
Identifiers	Yes	You, publicly available databases, government databases, data aggregators, affiliates, subsidiaries, agents or other producers, financial service providers, and other service providers	Respond to questions, requests, complaints, and emails; provide customer service; provide Services to you; set up, manage accounts; verify your identity; regulatory reporting; and update our records	Yes	Customer service, account set up, management, or servicing, data verification services, regulatory reporting requirements	Service providers that provide us with customer service, account set up, management, or servicing or data verification services, regulatory authorities	No	Not applicable	No	Generally 1 years but also subject to data retention schedules
Personal information described in California Civil Code Section 1798.80(e)	Yes	You, publicly available databases, government databases, data aggregators, affiliates, subsidiaries, agents or other producers, financial service providers, and other service providers	Respond to questions, requests and emails; provide customer service; set up, manage accounts; verify your identity; regulatory reporting; and update our records	Yes	Customer service, account management, servicing or data verification services, regulatory reporting requirements	Service providers that provide us with customer service, account management, or servicing or data verification services, regulatory authorities	No	Not applicable	No	Generally 1 years but also subject to data retention schedules
Characteristics of protected classifications under California or federal law	Yes	Directly from you or from service providers	Provide Services to you	Yes	Provide Services to you and regulatory reporting requirements	Entities that provide us with services to provide Services to you and regulatory authorities	No	Not applicable	No	Generally 1 years but also subject to data retention schedules
Commercial information	Yes	You directly, from your use of our Services, or from credit or consumer reporting agencies	Service your account	Yes	Policy administration and claims adjudication	Entities that provide us with services to provide Services to you and regulatory authorities	No	Not applicable	No	Generally 1 years but also subject to data retention schedules

Types of Personal Information	Do we collect it?	Categories of Sources	Purposes of Collection	Do we disclose it to third parties?	Purposes of Disclosure	Categories of Third Parties PI Disclosed To	Do we sell it to third parties?	Purposes of Selling	Do we Share for Behavioral Advertising?	Retention
Biometric information	Yes	You directly when you call our call centers	Detecting security incidents; fraud detection; authentication; protecting against and prosecuting malicious, deceptive, or illegal activity; verifying or maintaining the quality or safety of a service or device or improving a service or device	Yes	To assist in authentication and to service your account	Service providers that assist in authentication and to service your account	No	Not applicable	No	Generally 1 years but also subject to data retention schedules
Internet or other electronic network activity information	No	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Geolocation data	No	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Audio, electronic, visual, thermal, olfactory, or similar information	Yes	When you call our customer service call center	Improve our Services, quality assurance, analytics, or for security purposes	Yes	Improve customer service, loss prevention, authentication or fraud investigations	Entities that provide us with services to improve customer service; entities that provide us with loss prevention services; entities that provide authentication or fraud services	No	Not applicable	No	Generally 1 years but also subject to data retention schedules
Professional or employment-related information	No	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Education information	No	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Inferences	No	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

Types of Personal Information	Do we collect it?	Categories of Sources	Purposes of Collection	Do we disclose it to third parties?	Purposes of Disclosure	Categories of Third Parties PI Disclosed To	Do we sell it to third parties?	Purposes of Selling	Do we Share for Behavioral Advertising?	Retention
Sensitive personal information	Yes	You, your use of our Services, affiliates, subsidiaries, agents or other producers, or financial or other service providers	Maintain or service accounts, provide customer service, process and provide Services, verify customer information, regulatory purposes, or other similar services	Yes	Customer service, account management, financial services, quality and safety services, storage, and regulatory reporting	Entities that provide or assist us with customer service, account management, financial services, storage, and regulatory authorities	No	Not applicable	No	Generally 1 years but also subject to data retention schedules

For all categories of personal information, we may collect data directly from you, from third parties, including those to whom you have previously provided data, and from our service providers.

We collect and use personal information for business or commercial purposes. For all categories of personal information, these purposes may include auditing; detecting security incidents; protecting against and prosecuting illegal activity (such as fraud); ensuring the physical safety of individuals; debugging, short-term transient use of personal information; performing services on behalf of Spinnaker, such as maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing storage, or providing similar services on behalf of Spinnaker; undertaking internal technological research; verifying or maintaining the quality or safety of a service or device; improving a service or device; and monitoring and improving our Services' functionality. We combine the data that we collect in order to provide these functions.

We also collect and use personal information to comply with our legal obligations, resolve disputes, enforce our agreements, and for everyday servicing purposes.

For all categories of personal information, we may disclose your personal information to third parties in the event Spinnaker is involved in a merger, acquisition, or sale or transfer of all or part of its assets. We may also disclose all categories of personal information with our affiliates and subsidiaries. Spinnaker may be required to disclose your personal information to law enforcement, regulatory agencies, or litigants based on enforceable requests for this information. We may also need to disclose information based on fraud protection, credit risk reduction, or other legal purposes.

Please note that for all categories of personal information, we may also disclose your personal information to our service providers, partners, or collaborators we work with in the course of our business, agents or other insurance producers, any entity you instruct us to disclose your personal information to, and others.

Spinnaker retains personal information in accordance with our legal obligations, to defend against claims, or in compliance with our data retention policies and procedures. Also, we may retain your personal information in our backup or archived systems until the retention period of those systems expires.

16. You may have additional rights under various state privacy laws.

You may have the following rights with respect to your personal information:

- The right to a notice about our collection, use, disclosure, sale, or sharing of personal information about you. This statement is intended to satisfy this right.
- The right to request access to the personal information, including the specific pieces of personal information that Spinnaker has about you and personal information about any automated-decision making concerning you made by Spinnaker.
- The right to request that Spinnaker correct or amend your personal information.
- The right to request that we delete the personal information we have about you. We may not be required to delete personal information under particular circumstances.
- The right to opt out of the sale your personal information. You may have the right to opt out of cross-context behavioral advertisements.
- The right to ask us to limit our use of your sensitive personal information.
- The right to obtain a copy of your personal information in an easily understandable and portable format that you may also request be transmitted to another entity.
- The right to appeal Spinnaker's denial of your request to exercise a right herein.
- The right to opt out with respect to Spinnaker's use of automated decision-making technology, including profiling.
- The right to be free from retaliation for exercising these rights. We may, however, offer you incentives in return for your data. When you exercise your rights, you may lose access to these incentives, which can include discounts, coupons, or additional services.
- The right to use an authorized agent to submit a request on your behalf.
- The right to request a statement be placed in your file for others accessing your file if you disagree with Spinnaker's refusal to correct, amend, or delete your personal information with a concise statement of what you think is correct, relevant, or fair information and the reasons you disagree with Spinnaker's refusal to correct, amend, or deleted recorded personal information.

You may call us at 1-888-221-7742 or visit our [portal](#) to exercise your rights.

Your authorized agent may call us at 1-888-221-7742 to make a request on your behalf. You will be asked to confirm your identity with at least two identification factors, such as a verified email and phone number. If we cannot verify your identity, we will let you know and may deny the request. We must also receive a properly executed authorization form that adequately describes you, your designated agent, and the purpose of the designation. We may deny a request from an agent that does not submit proof that they have been authorized by you to act on your behalf. We may also require that you directly confirm with us that you provided the authorized agent permission to submit the request. The authorized agent must be a natural person or a business entity that is registered with the appropriate state regulatory agency to conduct business in the state they operate and must comply with the requirements of applicable laws.

17. Victims of domestic violence may have confidentiality rights.

New York State Insurance Law § 2612 prohibits insurers from discriminating against victims of domestic violence. This law also provides that if any person covered by an insurance policy delivers to the insurer a valid order of protection against the policyholder or other person covered by the policy, then the insurer is prohibited for the duration of the order from disclosing to the policyholder or other person the address and telephone number of

the, insured, or of any person or entity providing covered services to the insured. If a child is a covered person, then the right established by this section may be asserted by the child's parent or guardian.

Making a request:

To initiate a confidentiality request as it pertains to an order of protection, please submit a valid order of protection to the below listed address. You may use this [confidential communication request form](#), if you'd like:

Spinnaker Insurance Company
PO Box 240
Portsmouth, NH 03802
Toll Free Line: 1-(888) 221-7742

If the protected individual is a child, the parent or guardian may make the above request.

Revoking a request:

To revoke a confidentiality request, please contact our customer service at 1-(888) 221-7742.

18. We are based in the United States.

If you are visiting our Services from outside the United States, please be aware that we are based in the United States and the information we collect will be transferred to, processed, and stored on our servers in the United States in accordance with this privacy policy and applicable laws. The data protection laws and regulations applicable to your information transferred to the United States may be different from the laws in your country of residence.

19. We may change this privacy policy.

We may change this privacy policy from time to time. If we make material changes to this privacy policy, we will post the changes on our Services (or our Services that replace them) and provide you notice prior to the changes becoming effective either through the relevant Services or by some other means, such as email or through your account. Your continued use of our Services after such notice constitutes your consent to the changes. We encourage you to periodically review our privacy policy for the latest information on our privacy practices.

20. Spinnaker provides you with a Consumer Privacy Notice.

If you are a Spinnaker customer, then Spinnaker provides you with the Spinnaker Consumer Privacy Notice below.

21. Spinnaker provides you with a California Financial Information Privacy Act Notice.

If you are a Spinnaker customer in California, then Spinnaker provides you with the Spinnaker California Financial Information Privacy Act Notice below.

22. You may contact us.

If you have any questions about this privacy policy or our other information practices, please contact us at contact@Spinnaker.com; 1-888-221-7742; or Spinnaker Insurance Company, 1 Pluckemin Way, Suite 102, Bedminster, NJ 07921.

FACTS

WHAT SPINNAKER DOES WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.	
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: <ul style="list-style-type: none"> Name and date of birth Property information and property records Checking account information and credit-based insurance scores 	
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Spinnaker chooses to share; and whether you can limit this sharing.	
Reasons we can share your personal information	Does Spinnaker share?	Can you limit this sharing?
For our everyday business purposes — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes — to offer our products and services to you	No	No
For joint marketing with other financial companies	No	No
For our affiliates' everyday business purposes — information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes — information about your creditworthiness	No	We don't share
For our affiliates to market to you	No	We don't share
For nonaffiliates to market to you	No	We don't share
Questions?	Call toll-free 1-800-747-3214.	
Who we are		
Who is providing this notice?	Spinnaker Insurance Company and its insurance company subsidiaries	
What we do		
How does Spinnaker protect my personal information?	To protect your personal information from unauthorized access and use, we maintain physical, electronic, and procedural safeguards that comply with federal law. These measures include computer safeguards and secured files and buildings.	
How does Spinnaker collect my personal information?	We collect your personal information, for example, when you: <ul style="list-style-type: none"> apply for insurance or pay insurance premiums provide account information or give us your contact information file an insurance claim We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.	
Why can't I limit all sharing?	Federal law gives you the right to limit only <ul style="list-style-type: none"> sharing for affiliates' everyday business purposes – information about your creditworthiness affiliates from using your information to market to you sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. See below for more on your rights under state law.	

What happens when I limit sharing for an account I hold jointly with someone else?	Your choices will apply to everyone on your account.
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. <ul style="list-style-type: none"> ▪ Our affiliates include financial companies such as companies that share the Spinnaker, Wingsail, Masthead, or Hippo brand.
Nonaffiliates	nonfinancial companies. <ul style="list-style-type: none"> ▪ Spinnaker does not share with nonaffiliates so they can market to you.
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. <ul style="list-style-type: none"> ▪ Spinnaker doesn't jointly market.
Other Important Information	
<p>We will also comply with more restrictive state laws to the extent they apply.</p> <p>California Residents: We will not share your information with nonaffiliated third parties for their marketing purposes except with your express consent. California residents will also be provided an "Important Privacy Choices" notice explaining their rights under the California Financial Information Privacy Act.</p> <p>Nevada Residents: Nevada law allows us to make marketing calls to our existing customers listed on the National Do Not Call Registry. This notice is provided to you pursuant to state law. If you prefer not to receive marketing calls from us, you may be placed on our internal Do Not Call List by calling 1-888-221-7742. If you would like more information about our practices, you may call 1-888-221-7742. You may also contact the Nevada Attorney General's office: Bureau of Consumer Protection, Office of the Nevada Attorney General, 555 E. Washington St., Suite 3900, Las Vegas, NV 89101; Phone number: (702) 486-3132; email: aginfo@ag.nv.gov.</p> <p>Vermont Residents: We will not disclose information about your creditworthiness to our affiliates and will not disclose your personal information, credit report, or health information to nonaffiliated third parties to market to you, other than as permitted by Vermont law, unless you authorize us to make those disclosures.</p> <p>AZ, CA, CT, GA, IL, ME, MA, MN, MT, NV, NJ, NC, OH, OR, or VA Residents. The term "Information" means information we collect in connection with insurance transactions. You have the right to request access to, correction, amendment, and deletion of personal information that we have about you. Please contact us at compliance@spinnakerins.com or Spinnaker Insurance Company, 1 Pluckemin Way, Suite 102, Bedminster, NJ 07921 with a notarized letter and include your name, address, and your policy, contract, or account number, and describe the information you wish to access, delete, or correct. We may share your Information with nonaffiliates without your prior authorization as permitted or required by law, such as for purpose of conducting actuarial or research studies that comply with applicable law. We may share your Information with insurance regulatory authorities, law enforcement, consumer reporting agencies, auditors, and as permitted or required by law. Information we obtain from a report prepared by an insurance-support organization may be retained by that insurance-support organization and disclosed to others.</p>	

Important Privacy Choices for Consumers

**You have the right to control whether we share some of your personal information.
Please read the following information carefully before you make your choices below.**

Your Rights

You have the following rights to restrict the sharing of personal and financial information with our affiliates (companies we own or control) and outside companies that we do business with. Nothing in this form prohibits the sharing of information necessary for us to follow the law, as permitted by law, or to give you the best service on your account with us. This includes sending you information about some other products or services.

Your Choices

Restrict Information Sharing With Companies We Own or Control (Affiliates): Unless you say "No," we may share personal and financial information about you with our affiliated companies.

(—) NO, please do not share personal and financial information with your affiliated companies.

Restrict Information Sharing With Other Companies We Do Business With To Provide Financial Products And Services: Unless you say "No," we may share personal and financial information about you with outside companies we contract with to provide financial products and services to you.

(—) NO, please do not share personal and financial information with outside companies you contract with to provide financial products and services.

Time Sensitive Reply

You may make your privacy choice(s) at any time. Your choice(s) marked here will remain unless you state otherwise. However, if we do not hear from you, we may share some of your information with affiliated companies and other companies with whom we have contracts to provide products and services.

To exercise your choices, utilize any of the options below:

- (1) Call 1-800-747-3214, toll free; or
- (2) Complete the information needed below, sign, and return this form to us (you may want to make a copy for your records):
 - Mail to: Spinnaker Group, 1 Pluckemin Way, Suite 102, Bedminster, NJ 07921, Attn: Privacy Officer

Name: _____

Account Number(s): _____

Property Address: _____

Mailing Address: _____
(if different than property address)

Signature: _____ Date: _____