PLEASE READ THIS ENDORSEMENT CAREFULLY, AS IT MODIFIES THE POLICY.

CYBER LIABILITY AND DATA BREACH RESPONSE COVERAGE PART

Throughout this Coverage Part, the words “you” and “your” refer to the “named insured(s)” shown in the Declarations of this Coverage Part and any other person(s) or organization(s) qualifying as a “named insured” under this Coverage Part. The words “we”, “us”, and “our” refer to the company providing this insurance.

Paragraphs A, C, D, E, and F of SECTION I – INSURING AGREEMENTS provide coverage on a claims made and reported basis and apply only to claims first made and against the insured during the policy period or the optional extension period (if applicable) and reported to “us” during the policy period.

Paragraphs B and G of SECTION I – INSURING AGREEMENTS provide first party coverage on an incident discovered and reported basis and apply only to incidents first discovered and reported to “us” during the policy period.

SECTION I – INSURING AGREEMENTS

A. Information Security And Privacy Liability

“We” shall pay on behalf of the “insured”, “damages” and “claims expenses”, in excess of the “retention”, which the “insured” shall become legally obligated to pay because of any “claim”, including a “claim” for violation of a “privacy law”, for:

1. Theft, loss, or “unauthorized disclosure” of “personally identifiable information” or “third party information” that is in the care, custody or control of the “insured organization”, or a third party for whose theft, loss or “unauthorized disclosure” of “personally identifiable information” or “third party information” the “insured organization” is legally liable;

2. One or more of the following acts or incidents that directly result from a failure of “computer security” to prevent a “security breach”:
   a. The alteration, corruption, destruction, deletion, or damage to data stored on “computer systems”;
   b. The failure to prevent transmission of malicious code from “computer systems” to computer or network systems that are not owned, operated or controlled by an “insured”; or
   c. The participation by the “insured organization’s computer system” in a denial of service attack directed against computer or network systems that are not owned, operated or controlled by an “insured”;

3. The “insured organization’s” failure to timely disclose an incident described in paragraphs A.1. or A.2. in violation of any “breach notice law”;

4. Failure by the “insured” to comply with that part of a “privacy policy” that specifically:
   a. Prohibits or restricts the “insured organization’s” disclosure, sharing or selling of a person’s “personally identifiable information”;
   b. Requires the “insured organization” to provide access to “personally identifiable information” or to correct incomplete or inaccurate “personally identifiable information” after a request is made by a person; or
   c. Mandates procedures and requirements to prevent the loss of “personally identifiable information”;

Provided the “insured organization” must, at the time of such acts, errors or omissions have in force a “privacy policy” that addresses subsections 4(a) – (c) above that are relevant to such “claim”; or

5. Failure by the “insured” to administer:
   a. An identity theft prevention program required by regulations and guidelines promulgated pursuant to 15 U.S.C. §1681m(e), as amended; or
   b. An information disposal program required by regulations and guidelines promulgated pursuant to 15 U.S.C §1681W, as amended.

All acts, incidents, failures to timely disclose, failures to comply, thefts, losses, errors or omissions described in SECTION I – INSURING AGREEMENTS, A. Information Security And Privacy Liability must first take place on or after the Retroactive Date and before the end of the “policy period” to be eligible for coverage under SECTION I – INSURING AGREEMENTS, A. Information Security And Privacy Liability.
B. Privacy Breach Response Services

“We” shall provide to the “insured organization” “privacy breach response services” in excess of the “retention” because of an incident described in Paragraphs 1. and 2. of SECTION I – INSURING AGREEMENTS, A. Information Security and Privacy Liability.

“Privacy breach response services” means:
1. “Computer expert services”;
2. “Legal services”;
3. “Public relations and crisis management expenses”.

Paragraphs B(1) – (3) are subject to a monetary limit in excess of the “retention” noted in the Declarations.

4. “Notification services” to provide notification to:
   a. Individuals who are required to be notified by the “insured organization” under the applicable “breach notice law”; or
   b. Individuals, who at “our” discretion, have been affected by an incident in which their “personally identifiable information” has been subject to theft, loss, or “unauthorized disclosure” in a manner which compromises the security or privacy of such individual by posing a significant risk of financial, reputational or other harm to the individual;

5. “Call center services”; and
6. “Breach resolution and mitigation services”;

Paragraphs B(4) – (6) are subject to a monetary limit in excess of the “retention” noted in the Declarations.

“Privacy breach response services” also includes assistance from the Beazley Breach Response Services Team and access to education and loss control information at no charge. “Privacy breach response services” will be provided subject to the terms and conditions of this Coverage Part and the conditions applicable set forth more fully in SECTION XII – CONDITIONS APPLICABLE TO PRIVACY BREACH RESPONSE SERVICES AND COVERAGE and shall not include any internal salary or overhead expenses of the “insured organization”.

C. Regulatory Defense And Penalties

“We” shall pay on behalf of the “insured”, “claims expenses” and “penalties” in excess of the “retention”, which the “insured” shall become legally obligated to pay because of any “claim” in the form of a “regulatory proceeding”, caused by an incident described in Paragraphs 1., 2., and 3. of SECTION I – INSURING AGREEMENTS, A. Information Security and Privacy Liability that first takes place on or after the “retroactive date” and before the end of the “policy period”.

D. Website Media Content Liability

“We” shall pay on behalf of the “insured”, “damages” and “claims expenses”, in excess of the “retention”, which the “insured” becomes legally obligated to pay 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 the “insured organization’s” display of “media material” on its web site or on social media web pages created and maintained by or on behalf of the “insured organization”:

1. Defamation, libel, slander, trade libel, infliction of emotional distress, outrage, outrageous conduct, or other tort related to disparagement or harm to the reputation or character of any person or organization;
2. A violation of the rights of privacy of an individual, including false light and public disclosure of private facts;
3. Invasion or interference with an individual’s right of publicity, including commercial appropriation of name, persona, voice or likeness;
4. Plagiarism, piracy, misappropriation of ideas under implied contract;
5. Infringement of copyright;
6. Infringement of domain name, trademark, trade name, trade dress, logo, title, metatag, or slogan, service mark, or service name; or
7. Improper deep-linking or framing within electronic content.

E. PCI Fines, Expenses And Costs

“We” shall indemnify the “insured” for “PCI Fines, Expenses, and Costs”, in excess of the “retention”, which the “insured” shall become legally obligated to pay. Coverage under SECTION I – INSURING AGREEMENTS, E. PCI Fines, Expenses And Costs is sublimited to the amount set forth in the Declarations. “We” have no duty to defend any “claim” or to pay any “claims expenses” associated with a “claim” brought under SECTION I – INSURING AGREEMENTS, E. PCI Fines, Expenses And Costs.

F. Cyber Extortion

“We” shall reimburse the “insured” for “cyber extortion loss”, in excess of the “retention”, which the “insured” pays as a direct result of an “extortion threat” first made against the “insured” on or after the “retroactive date” and before the end of the “policy period” by a person, other than the “insured’s” employees, directors, officers, principals, trustees, governors, “managers”, members, management committee members, members of the management board, partners, contractors, outsourcers, or any person in collusion with any of the foregoing. Coverage under this Insuring Agreement is subject to the applicable conditions and reporting requirements,
including those set forth in SECTION XV, OBLIGATIONS IN THE EVENT OF AN EXTORTION THREAT.
Coverage under SECTION I – INSURING AGREEMENTS, F. Cyber Extortion is sublimited to the amount set forth in the Declarations.

G. First Party Data Protection
“We” shall reimburse the “insured” for “data protection loss” in excess of the “retention”, which the “insured” pays as a direct result of one or more of the following that first takes place on or after the “retroactive date” and before the end of the “policy period”:
1. alteration, corruption, destruction, deletion or damage to a “data asset”, or
2. inability to access a “data asset”, or

and is directly caused by a failure of “computer security” to prevent a “security breach”; provided that such “security breach” must take place on or after the “retroactive date” and before the end of the “policy period”.
Coverage under SECTION I – INSURING AGREEMENTS, G. is sublimited to the amount set forth in the Declarations.

SECTION II – DEFENSE AND SETTLEMENT OF CLAIMS
A. “We” shall have the right and duty to defend:
1. Any “claim” against the “insured” seeking “damages” even if any of the allegations of the “claim” are groundless, false or fraudulent; or
2. Under SECTION I – INSURED AGREEMENTS, C. Regulatory Defense And Penalties, any “claim” in the form of a “regulatory proceeding”.

Selection of defense counsel shall be mutually agreed upon between “us” and the “named insured”, but in the absence of such agreement, “our” decision shall be final.

B. With respect to any “claim” against the “insured” seeking “damages” or “penalties”, “we” will pay “claims expenses” incurred with their prior written consent. The Limit of Liability available to pay “damages” and “penalties” shall be reduced and may be completely exhausted by payment of “claims expenses”. “Damages”, “penalties”, and “claims expenses” shall be applied against the each “claim retention” payable by the “insured”.

C. If the “insured” refuses to consent to any settlement or compromise recommended by “us” and acceptable to the claimant and elects to contest the “claim”, “our” liability for any “damages”, “penalties”, and “claims expenses” shall not exceed the lesser of:
1. The amount for which the “claim” could have been settled, less the remaining “retention”, plus the “claims expenses” incurred up to the time of such refusal; or
2. The applicable Limit of Liability whichever is less, and “we” have the right to withdraw from further defense by tendering control of said defense to the “insured”. The portion of any proposed settlement or compromise that requires the “insured” to cease, limit or refrain from actual or alleged infringing or otherwise injurious activity or is attributable to future royalties or other amounts that are not “damages” (or “penalties” for “claims”) covered under SECTION I – INSURED AGREEMENTS, C. Regulatory Defense And Penalties shall not be considered in determining the amount for which a “claim” could have been settled.

SECTION III – WHO IS AN INSURED
Whether expressed in singular or plural, “insured” shall mean:
A. The “named insured” and any “subsidiaries” of the “named insured” (together the “insured organization”); 
B. A director, manager of a limited liability company (“manager”) or officer of the “insured organization”, but only with respect to the performance of their duties as such on behalf of the “insured organization”;
C. An employee of the “insured organization”, but only for work done while acting within the scope of their employment and related to the conduct of the “insured organization’s” business;
D. A principal if the “named insured” is a sole proprietorship, or a partner if the “named insured” is a partnership, but only with respect to the performance of their duties as such on behalf of the “insured organization”;
E. Any person previously qualified as an “insured” under Paragraphs B., C., or D. of SECTION III – WHO IS AN INSURED prior to the termination of the required relationship with the “insured organization”, but only with respect to the performance of their duties as such on behalf of the “insured organization”.

SECTION IV – EXCLUSIONS
This insurance does not apply to any “claim” or “loss”:
A. Arising out of or resulting from any contractual liability or obligation, or arising out of or resulting from breach of contract or agreement either oral or written. However, this exclusion will not apply:
1. Only with respect to the coverage provided pursuant to Paragraph 1. of SECTION I – INSURING AGREEMENTS, A. Information Security And Privacy Liability, to any obligation of the “insured” organization to maintain the confidentiality or security of “personally identifiable information” or of “third party information”;
2. Only with respect to Paragraph 4. of SECTION I – INSURING AGREEMENTS, D. Website Media Content Liability, for misappropriation of ideas under implied contract; or
3. To the extent the “insured” would have been liable in the absence of such contract or agreement;

B. Arising out of or resulting from any liability or obligation under a “merchant services agreement” except this exclusion does not apply to “PCI Fines, Expenses, and Costs” covered under SECTION I – INSURING AGREEMENTS, E. PCI Fines, Expenses, and Costs, or to “computer expert services” or “legal services” covered under SECTION I – INSURING AGREEMENTS, B. Privacy Breach Response Services.

C. Arising out of or resulting from any actual or alleged false, deceptive or unfair trade practices; however, this exclusion does not apply to:
   1. Any “claim” covered under Paragraphs 1., 2., or 3. of SECTION I – INSURING AGREEMENTS, A. Information Security And Privacy Liability or SECTION I – INSURING AGREEMENTS, C. Regulatory Defense and Penalties;
   or

D. Arising out of or resulting from the actual or alleged unlawful collection, acquisition or “retention” of “personally identifiable information” (except as otherwise covered under Paragraph 5. of SECTION I – INSURING AGREEMENTS, A. Information Security And Privacy Liability) or other personal information by, on behalf of, or with the consent or cooperation of the “insured organization”; or the failure to comply with a legal requirement to provide individuals with the ability to assent to or withhold assent (e.g. opt-in or opt-out) from the collection, disclosure or use of “personally identifiable information”; provided that this exclusion shall not apply to the actual or alleged unlawful collection, acquisition or “retention” of “personally identifiable information” by a person or entity that is not a “related party” and without the knowledge of the “insured organization”.

E. Arising out of or resulting from any act, error, omission, incident, failure of “computer security”, or “security breach” committed or occurring prior to the inception date of this Coverage Part:
   1. If any member of the “control group” on or before the “continuity date” knew or could have reasonably foreseen that such act, error or omission, incident, failure of “computer security”, or “security breach” might be expected to be the basis of a “claim” or “loss”; or
   2. In respect of which any “insured” has given notice of a circumstance, which might lead to a “claim” or “loss”, to the insurer of any other policy in force prior to the inception date of this Coverage Part.

F. Arising out of or resulting from any related or continuing acts, errors, omissions, incidents or events, where the first such act, error, omission, incident or event was committed or occurred prior to the “retroactive date.”

G. Arising out of or resulting from any actual or alleged theft of or “unauthorized disclosure” of data; under Paragraph 2. of SECTION I – INSURING AGREEMENTS, A. Information Security And Privacy Liability

H. In connection with or resulting from a “claim” brought by or on behalf of the Federal Trade Commission, the Federal Communications Commission, or any other state, federal, local or foreign governmental entity, in such entity’s regulatory or official capacity; provided, this exclusion shall not apply to an otherwise covered “claim” under SECTION I – INSURING AGREEMENTS, C. Regulatory Defense and Penalties or to the providing of “privacy breach response services” under SECTION I – INSURING AGREEMENTS, B. Privacy Breach Response Services to the extent such services are legally required to comply with a “breach notice law”.

I. Arising out of or resulting from a “claim” by or on behalf of one or more “insureds” under this coverage against any other “insured” or “insureds” under this Coverage; provided this exclusion shall not apply to an otherwise covered “claim” under Paragraphs 1., 2., or 3. of SECTION I – INSURING AGREEMENTS, A. Information Security And Privacy Liability made by a current or former employee of the “insured organization”;

J. Arising out of or resulting from:
   1. Any “claim” made by any business enterprise in which any “insured” has greater than a fifteen percent (15%) ownership interest or made by any parent company or other entity which owns more than fifteen percent (15%) of the “named insured”; or
   2. The “insured’s” activities as a trustee, partner, member, “manager”, officer, director or employee of any employee trust, charitable organization, corporation, company or business other than that of the “insured organization”;

K. Arising out of or resulting from:
   1. The actual or alleged obligation to make licensing fee or royalty payments;
   2. Any costs or expenses incurred or to be incurred by the “insured” or others for the reprinting, reposting, recall, removal or disposal of any “media material” or any other information, content or media, including any media or products containing such “media material”, information, content or media;
   3. Any “claim” brought by or on behalf of any intellectual property licensing bodies or organizations;
   4. The actual or alleged inaccurate, inadequate or incomplete description of the price of goods, products or services, cost guarantees, cost representations, or contract price estimates, the authenticity of any goods, products or services, or the failure of any goods or services to conform with any represented quality or performance;
   5. Any actual or alleged gambling, contest, lottery, promotional game or other game of chance; or
   6. Any “claim” made by or on behalf of any independent contractor, joint venture or venture partner arising out of or resulting from disputes over ownership of rights in “media material” or services provided by such independent contractor, joint venture or venture partner;
L. With respect to SECTION I – INSURING AGREEMENTS F. Cyber Extortion and G. Data Protection Loss arising out of or resulting from any criminal, dishonest, fraudulent, or malicious act, error or omission, any “security breach”, “extortion threat”, or intentional or knowing violation of the law, if committed by any member of the “control group” or any person in participation or collusion with any member of the “control group”;

M. With respect to SECTION I – INSURING AGREEMENTS G. Data Protection Loss: Arising out of or resulting from:

1. Any failure or malfunction of electrical or telecommunications infrastructure or services, provided that this exclusion shall not apply to any otherwise covered “claim” or “loss” arising out of failure of “computer security” to prevent a “security breach” that was solely caused by a failure or malfunction of telecommunications infrastructure or services under the “insured’s” direct operational control;
2. Fire, flood, earthquake, volcanic eruption, explosion, lighting, wind, hail, tidal wave, landslide, act of God or other physical event; or
3. Any satellite failures.

N. With respect to SECTION I – INSURING AGREEMENTS F. Cyber Extortion arising out of or resulting from:

1. any threat to physically harm or kidnap any person; or
2. any threat to harm, take, or transfer property other than any “data asset”, even if such threat is made in conjunction with a threat to a “data asset” or by carrying out such threat to, harm, theft, or transfer, a “data asset” may be damaged, corrupted, altered, taken, disseminated or transferred;

O. Arising out of or resulting from any seizure, nationalization, confiscation, or destruction of “computer systems” or “data assets” by order of any governmental or public authority;

P. Arising out of or resulting from, directly or indirectly occasioned by, happening through or in consequence of: war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority;

SECTION V – LIMIT OF LIABILITY AND COVERAGE
A. The “policy aggregate limit of liability” set forth in the Declarations is “our” combined total limit of liability for all “damages”, “penalties”, “PCI Fines, Expenses, and Costs”, “crisis management and public relations expenses”, “cyber extortion loss”, “data protection loss”, and “claims expenses” payable under this Coverage Part.

B. The Regulatory Defense and Penalties sublimit of liability stated in the Declarations is the aggregate sublimit of liability payable under SECTION I – INSURING AGREEMENTS, C. Regulatory Defense and Penalties of this Coverage Part and is part of and not in addition to the “policy aggregate limit of liability”.

C. The “PCI Fines, Expenses, and Costs” sublimit of liability stated in the Declarations is the aggregate sublimit of liability payable under SECTION I – INSURING AGREEMENTS, E. PCI Fines, Expenses, and Costs of this Coverage Part and is part of and not in addition to the “policy aggregate limit of liability”.

D. The “Cyber Extortion” and “First Party Data Protection” sublimit of liability stated in the Declarations is the aggregate sublimit of liability payable under SECTION I – INSURING AGREEMENTS, F. Cyber Extortion and G. First Party Data Protection of this Coverage Part and is part of and not in addition to the “policy aggregate limit of liability”.

E. Neither the inclusion of more than one “insured” under this Coverage Part, nor the making of “claims” by more than one person or entity shall increase the Limit of Liability.

F. The Limit of Liability for the “optional extension period” shall be part of and not in addition to the “policy aggregate limit of liability”.

G. “We” shall not be obligated to pay any “damages”, “penalties”, or “claims expenses”, or to undertake or continue defense of any suit or proceeding after the “policy aggregate limit of liability” has been exhausted by payment of “damages”, “penalties”, “PCI Fines, Expenses and Costs” “crisis management and public relations expenses”, “cyber extortion loss”, “data protection loss” or “claims expenses”, or after deposit of the “policy aggregate limit of liability” in a court of competent jurisdiction. Upon such payment, “we” shall have the right to withdraw from further defense of any “claim” under this Coverage Part by tendering control of said defense to the “insured”

H. Unless otherwise specified in this Coverage Part, “privacy breach response services” will be provided by a service provider selected by “us” in accordance with SECTION XII CONDITIONS APPLICABLE TO PRIVACY BREACH RESPONSE SERVICES AND COVERAGE.

I. The policy aggregate limit of liability payable under SECTION I – INSURING AGREEMENTS, B. Privacy Breach Response Services is separate from and in addition to the “policy aggregate limit of liability” set for in this Section V – LIMIT OF LIABILITY AND COVERAGE, Paragraph A.
J. The "notified individuals" limit stated in the Declarations is the maximum total number of "notified individuals" to whom notification will be provided or attempted for all incidents or series of related incidents giving rise to an obligations to provide "notification services", "call center services" or "breach resolution and mitigation services.

K. The aggregate limit of coverage stated for "computer expert services", "legal services", and "public relations and crisis management services" in the Declarations is the aggregate limit of coverage for all "computer expert services", "legal services" and "crisis management and public relations services" combined. This is a separate limit, apart from, and in addition to the policy aggregate limit of liability.

L. If the total number of notifications made pursuant to Paragraph 3. of SECTION I – INSURING AGREEMENTS, B. Privacy Breach Response Services aggregates to more than the "notification services" Limit of Coverage stated in the Declarations, the "insured organization" will be responsible for paying for "privacy breach response services" with respect to any excess notification, and such costs will not be covered under this Coverage Form. If an incident involves notifications made pursuant to Paragraph 3. of SECTION I – INSURING AGREEMENTS, B. Privacy Breach Response Services both within the "notification services" Limit of Coverage stated in the Declarations and in excess of such limit, all excess notifications will be provided by the same service provider that provides "notification services" covered under this Coverage Form, and the costs will be allocated between "us" and the "insured organization" pro rata based on the number of covered and non-covered notifications.

M. To the extent that costs to provide Privacy Breach Response Services are covered pursuant to a "claim" described in Paragraph D.4. of SECTION XI -- DEFINITIONS., such costs shall be covered solely under SECTION I – INSURING AGREEMENTS, A. Information Security and Privacy Liability.

SECTION VI – RETENTION

A. The each "claim" "retention" amount set forth in the Declarations applies separately to each incident, event or related incidents or events, giving rise to a "claim". The "retention" shall be satisfied by monetary payments by the "named insured" of "damages", "claims expenses", "crisis management and public relations expenses", "penalties", "cyber extortion loss", "data protection loss", or "PCI Fines, Expenses and Costs".

B. For all "computer expert services", "legal services", and "public relations and crisis management services", the "retention" amounts set forth in the Declarations apply separately to each incident, event or related incidents or events, giving rise to an obligation to provide such services; and the Each Incident "retention" shall be satisfied by monetary payments by the "named insured" for such services.

C. For all "notification services", "call center services" and "breach resolution and mitigation services" for each incident, the notified individuals sublimit set forth in the Declarations applies separately to each incident, event or related incidents or events, giving rise to an obligation to provide such services.

D. In the event that "damages", "claims expenses", "penalties" or "PCI Fines, Expenses and Costs" arising out of a "claim" are subject to more than one "retention", the applicable "retention" amounts shall apply to such "damages", "claims expenses", "penalties" or "PCI Fines, Expenses and Costs", provided that the sum of such "retention" amounts shall not exceed the largest applicable "retention" amount.

E. Satisfaction of the applicable "retention" is a condition precedent to the payment by "us" of any amounts or providing of any services hereunder, and "we" shall be liable only for the amounts in excess of such "retention" subject to "our" total liability not exceeding the "policy aggregate limit" or Limits of Coverage for "privacy breach response services" set forth in the Declarations. The "named insured" shall make direct payments within the "retention" to appropriate other parties designated by "us".

SECTION VII – EXTENSION PERIODS

A. AUTOMATIC EXTENSION PERIOD

We will provide a fourteen (14) day "automatic extension period" in the event of termination of this Coverage Part for any reason except the non-payment of premium.

B. OPTIONAL EXTENSION PERIOD

1. "We" will provide an "optional extension period" as described below in the event of termination of this Coverage Part for any reason except the non-payment of premium.

2. The "optional extension period" does not extend the policy period or change the scope of the coverage provided. The "optional extension period" only extends the "claims" reporting period.

3. A "claim" first made against any "insured" and reported to "us" during the "optional extension period" will be deemed to have been made on the last day of the policy period provided that the "claim" is for any act, error, or omission committed on or after the "retroactive date" and before the end of the "policy period".

4. The Limit of Liability for the "optional extension period" shall be part of, and not in addition to, the applicable Limit of Liability for the "policy period". The purchase of the "optional extension period" does not in any way increase the "policy aggregate limit of liability" or any sublimit of liability.

5. The "optional extension period" does not apply to SECTION I – INSURING AGREEMENTS, B. Privacy Breach Response Services.
6. “You” must give us a written request within thirty (30) days of “your” election of the “optional extension period”. Payment of the full additional premium for the “optional extension period” endorsement is due within thirty (30) days of the termination of this Coverage Part. If notice of election and payment for the “optional extension period” is not given to “us” within such thirty (30) day period, there shall be no right to purchase the “optional extension period”.  

7. At the commencement of the “optional extension period” the entire premium shall be deemed earned, and in the event the “named insured” terminates the “optional extension period” for any reason prior to its natural expiration, “we” will not be liable to return any premium paid for the “optional extension period”.  

SECTION VIII – NOTICE OF CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM  

A. If any “claim” is made against the “insured” the “insured” shall forward as soon as practicable to “us” written notice of such “claim” in the form of a facsimile, email or express or certified mail together with every demand, notice, summons or other process received by the “insured” or the “insured’s” representative.  

B. With respect to SECTION I – INSURING AGREEMENTS, B. Privacy Breach Response Services, for a legal obligation to comply with a “breach notice law” because of an incident described in Paragraph 1. or 2. of SECTION I – INSURING AGREEMENTS, A. Information Security And Privacy Liability, such incident or reasonably suspected incident must be reported as soon as practicable during the “policy period”, or during the optional extended reporting period, if applicable, after discovery by the “insured”.  

C. If during the “policy period”, or optional extension period, if applicable, the “insured” becomes aware of any circumstance that could reasonably be the basis for a “claim” it may give written notice to “us” in the form of a facsimile, email or express or certified mail as soon as practicable during the “policy period”. Such a notice must include:  

1. The specific details of the act, error, omission, or “security breach” that could reasonably be the basis for a “claim”;  
2. The injury or damage which may result or has resulted from the circumstance; and  
3. The facts by which the “insured” first became aware of the act, error, omission or “security breach”.  

Any subsequent “claim” made against the “insured” arising out of such circumstance which is the subject of the written notice will be deemed to have been made at the time written notice complying with the above requirements was first given to “us”.  

An incident or reasonably suspected incident reported to “us” during the “policy period”, or optional extended reporting period, if applicable and in conformance with Paragraph B of SECTION VIII – NOTICE OF CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM shall also constitute notice of a circumstance under this Paragraph C.  

D. A “claim” or legal obligation under Paragraphs A. or B. of SECTION VIII – NOTICE OF CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM shall be considered to be reported to “us” when written notice is first received by “us” in the form of a facsimile, email or express or certified mail or email of the “claim” or legal obligation, or of an act, error, or omission, which could reasonably be expected to give rise to a “claim” if provided in compliance with Paragraph C. of SECTION VIII – NOTICE OF CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM.  

E. With respect to SECTION I INSURING AGREEMENT F – Cyber Extortion, in the event of an “extortion threat” to which this insurance applies, the “insured” shall notify “us” by calling Tel: (866) 567-8570 immediately upon receipt of any “extortion threat”, and shall thereafter also provide written notice by facsimile, email or express mail within five (5) days following the “extortion threat”.  

SECTION IX – OTHER INSURANCE  

A. If any covered “claim” or “loss” is insured by any other valid policy, then this Coverage Part shall apply only in excess of the amount of any deductible, retention and limit of insurance under such other policy, whether such other policy is stated to be primary, contributory, excess, contingent or otherwise, unless such other policy is written specifically excess of this Coverage Part by reference in such other policy to this Coverage Part's policy number.  

B. When this Coverage Part is excess, we shall have no duty to defend the “insured” against any “claim” if any other insurer has a duty to defend the “insured” against that “suit”. If no other insurer defends, we will undertake to do so, but we will be entitled to the “insured’s” rights against all those other insurers.  

The “named insured” shall be considered the agent of all “insureds” and shall act on behalf of all “insureds” with respect to the giving of or receipt of all notices pertaining to this Coverage Part.  

SECTION X – DEFINITIONS
A. “Breach notice law” means any statute or regulation that requires notice to persons whose “personally identifiable information” was accessed or reasonably may have been accessed by an unauthorized person.

B. “Breach resolution and mitigation services” means a credit monitoring, identity monitoring or other solution selected from the product list “we” offer “notified individuals”. The product offered to “notified individuals” will be selected by “us” in consultation with the “insured organization” and in accordance with SECTION XII CONDITIONS APPLICABLE TO PRIVACY BREACH RESPONSE SERVICES AND COVERAGE.

C. “Call center services” means the provision of a call center to answer calls during standard business hours for a period of ninety (90) days following notification (or longer if required by applicable law or regulation) of an incident for which notice is provided pursuant to Paragraph 3. of SECTION I – INSURING AGREEMENTS, B. Privacy Breach Response Services.

D. “Claim” means:
   1. A written demand received by any “insured” for money or services; including service of a suit or institution of regulatory or arbitration proceedings;
   2. With respect to coverage provided under SECTION I – INSURING AGREEMENTS, C. Regulatory Defense And Penalties only, institution of a “regulatory proceeding” against any “insured”;
   3. A written request or agreement to toll or waive a statute of limitations relating to a potential “claim” described in Paragraph 1. above; and
   4. With respect to coverage provided under Paragraph 1. of SECTION I – INSURING AGREEMENTS, A. Information Security And Privacy Liability only, a demand received by any “insured” to fulfill the “insured organization’s” contractual obligation to provide notice of an incident (or reasonably suspected incident) described in Paragraph 1. of SECTION I – INSURING AGREEMENTS, A. Information Security And Privacy Liability pursuant to a “breach notice law”.

E. “Claims expenses” means:
   1. Reasonable and necessary fees charged by an attorney designated pursuant to Paragraph A. of SECTION II – DEFENSE AND SETTLEMENT OF CLAIMS.
   2. All other legal costs and expenses resulting from the investigation, adjustment, defense and appeal of a “claim”, suit, or proceeding arising in connection therewith, or circumstance which might lead to a “claim”, if incurred by “us”, or by the “insured” with the prior written consent of “us”; and
   3. The premium cost for appeal bonds for covered judgments or bonds to release property used to secure a legal obligation, if required in any “claim” against an “insured” provided that “we” shall have no obligation to appeal or to obtain bonds.

   “Claims expenses” do not include any salary, overhead, or other charges by the “insured” for any time spent in cooperating in the defense and investigation of any “claim” or circumstance that might lead to a “claim” notified under this Coverage Part, or costs to comply with any regulatory orders, settlements or judgments.

F. “Computer expert services” means costs for:
   1. A computer security expert to determine the existence and cause of an actual or suspected electronic data breach which may require the “insured organization” to comply with a “breach notice law” and to determine the extent to which such information was accessed by an unauthorized person or persons;
   2. A Payment Card Industry (PCI) Forensic Investigator that is approved by the PCI Security Standards Council and is retained by the “insured organization” in order to comply with the terms of a “merchant services agreement” to investigate the existence and extent of an actual or suspect compromise or credit card data; and in “our” discretion, where a computer security expert described in Paragraph 1. above has not been retained, for a computer security expert to provide advice and oversight in connection with the investigation conducted by the PCI Forensic Investigator; and
   3. A computer security expert services which amount is part of and not in addition to the combined aggregate limit of coverage for all “computer expert services”, “legal services”, and “public relations and crisis management expenses” stated in the Declarations to demonstrate the “insureds” ability to prevent a future electronic data breach as required by a “merchant services agreement”.

“Computer expert services” will be provided in accordance with the terms and conditions set forth in this Coverage Part and will be provided by a service provider selected by the “insured organization” in consultation with “us” from the list of service providers “we” provide.
G. “Computer security” means software, computer or network hardware devices, as well as the “insured organization’s” written information security policies and procedures, the function or purpose of which is to prevent “unauthorized access or use”, a denial of service attack against “computer systems”, infection of “computer systems” by malicious code or transmission of malicious code from “computer systems”. “Computer security” includes anti-virus and intrusion detection software, firewalls and electronic systems that provide access control to “computer systems” through the use of passwords, biometric or similar identification of authorized users.

H. “Computer systems” means computers and associated input and output devices, data storage devices, networking equipment, and back up facilities:
   1. Operated by and either owned by or leased to the “insured organization”; or
   2. Systems operated by a third party service provider and used for the purpose of providing hosted computer application services to the “insured organization” or for processing, maintaining, hosting or storing the “insured organization’s” electronic data, pursuant to written contract with the “insured organization” for such services.

I. “Continuity date” means:
   1. The date stated in the Declarations that coverage was first written with respect to the “named insured” and any “subsidiaries” acquired before such date. Any litigation initiated before this date is not subject to coverage under this Coverage Form even if the allegations were not part of a potentially covered claim.

J. “Control group” means the individuals holding the following positions in the “insured organization”:
   1. President;
   2. Members of the Board of Directors;
   3. Executive Officers, including the Chief Executive Officer, Chief Operating Officer, and Chief Financial Officer; General Counsel, Chief Information Officer, Chief Security Officer, Chief Privacy Officer;
   4. Staff attorneys employed by the “insured organization”
   5. “Manager”; and
   6. Any individual in a substantially similar position or which substantially similar responsibilities as those referenced above.

K. “Cyber extortion loss” means:
   1. Any “extortion payment” that has been made under duress by or on behalf of the “insured” with “our” prior written consent, but solely to prevent or terminate an “extortion threat” and in an amount that does not exceed the covered “damages” that would have been incurred had the “extortion payment” not been paid;
   2. An otherwise covered “extortion payment” that is lost in transit by actual destruction, disappearance or wrongful abstraction while being conveyed by any person authorized by or on behalf of the “insured” to make such conveyance; and
   3. Fees and expenses paid by or on behalf of the “insured” for security consultants retained with “our” prior written approval, but solely to prevent or terminate an “extortion threat”.

L. “Damages” means a monetary judgment, award or settlement; provided that the term “damages” shall not include or mean:
   1. Future profits, restitution, disgorgement of unjust enrichment or profits by an “insured”, or the costs of complying with orders granting injunctive or equitable relief;
   2. Return or offset of fees, charges, or commissions charged by or owned to an “insured” for goods or services already provided or contracted to be provided;
   3. Any damages which are a multiple of compensatory damages, fines, taxes or loss of tax benefits, sanctions or penalties;
   4. Punitive or exemplary damages, unless insurable by law in any applicable venue that most favors coverage for such punitive or exemplary damages;
   5. Discounts, coupons, prizes, awards or other incentives offered to the “insured’s” customers or clients;
   6. Liquidated damages to the extent that such damages exceed the amount for which the “insured” would have been liable in the absence of such liquidated damages agreement; or
   7. Any amounts for which the “insured” is not liable, or for which there is no legal recourse against the “insured”.

M. “Data asset” means any software or electronic data that exists in “computer systems” and is subject to regular back up procedures, including computer programs, applications, account information, customer information, private or personal information, marketing information, financial information and any other information maintained by the Insured Organization in its ordinary course of business.

N. “Data protection loss” means:
   1. With respect to any “data asset” that is altered, corrupted, destroyed, deleted or damaged the actual, reasonable and necessary costs and expenses incurred by the “insured” to restore a “data asset” from back-ups or from originals or to gather, assemble and recollect such “data asset” from other sources to the level or condition in which it existed immediately prior to its alteration, corruption, destruction, deletion or damage; or
   2. With respect to any “data asset” that the “insured” is unable to access, the lesser of the actual, reasonable and necessary costs and expenses incurred by the “insured organization” to:
(a) Regain access to such "data asset"; or

(b) restore such "data asset" from back-ups or originals or gather, assemble and recollect such "data asset" from other sources, to the level or condition in which it existed immediately prior to the "insured's" inability to access it;

Provided that if such "data asset" cannot reasonably be accessed, restored, gathered, assembled or recollected, then "data protection loss" means the actual, reasonable and necessary costs and expenses incurred by the "insured" to reach this determination.

Provided further that "data protection loss" shall not exceed, and shall not mean, any amount in excess of the amount by which the net profit before income taxes of the "insured" would have decreased had the "insured" failed to restore, gather, assemble or recollect as set forth in sub-paragraphs M.1. and M.2. above.

A "data protection loss" will be deemed to occur at the time such alteration, corruption, destruction, deletion or damage to or inability to access a "data asset" is first discovered by the "insured". All "data protection loss" that arises out of the same or a continuing "security breach", from related or repeated "security breaches", or from multiple "security breaches" resulting from a failure of "computer security" shall be deemed to be a single "data protection loss".

"Data protection loss" shall not mean, and there shall be no coverage under SECTION I – INSURING AGREEMENTS, G. First Party Data Protection for:

1. Costs or expenses incurred by the "insured" to identify or remediate software program errors or vulnerabilities or update, replace, restore, gather, assemble, reproduce, recollect or enhance a "data asset" or "computer systems" to a level beyond that which existed prior to the alteration, corruption, destruction, deletion or damage of such "data asset";

2. Costs or expenses to research or develop any "data asset", including but not limited to trade secrets or other proprietary information;

3. the monetary value of profits, royalties, or lost market share related to a "data asset", including but not limited to trade secrets or other proprietary information or any other amount pertaining to the value of the "data asset";

4. loss arising out of any liability to any third party for whatever reason; or

5. legal costs or legal expenses of any type.

O. "Denial of service attack" means an attack intended by the perpetrator to overwhelm the capacity of a "computer system" by sending an excessive volume of electronic data to such "computer system" in order to prevent authorized access to such "computer system".

P. "Dependent business" means any third party service provider that provides hosted computer application services to the "insured" or processes, maintains, hosts or stores the "insured's" electronic data, pursuant to written contract with the "insured" for such services. "Extortion payment" means cash, marketable goods or services demanded to prevent or terminate an "extortion threat".

Q. "Extortion threat" means a threat to breach "computer security" in order to:

1. Alter, destroy, damage, delete or corrupt any "data asset";

2. Prevent access to "computer systems" or a "data asset", including a "denial of service attack" or encrypting a "data asset" and withholding the decryption key for such "data asset";

3. Perpetrate a theft or misuse of a "data asset" on "computer systems" through external access;

4. Introduce "malicious code" into "computer systems" or to third party computers and systems from "computer systems";

5. Interrupt or suspend "computer systems";

Unless an "extortion payment" is received from or on behalf of the "insured".

Multiple related or continuing "extortion threats" shall be considered a single "extortion threat" for purposes of this insurance and shall be deemed to have occurred at the time of the first such "extortion threat".

R. "Legal services" means fees charged by an attorney:
1. To determine the applicability of and actions necessary for the “insured organization” to comply with “breach notice laws” due to an actual or reasonably suspected theft, loss or “unauthorized disclosure” of “personally identifiable information”;
2. To provide necessary legal advice to the “insured organization” in responding to actual or suspected theft, loss or “unauthorized disclosure” of “personally identifiable information”, and
3. To advise the “insured organization” in responding to credit card system operating regulation requirements for any actual or suspected compromise of credit card data that is required to be reported to the “insured organization’s” merchant bank under the terms of a “merchant services agreement”, but “legal services” does not include fees incurred in any actual or threatened legal proceeding, arbitration or mediation, or any advice in responding to credit card system operating regulation in connection with an assessment of “PCI Fines, Expenses, and Costs”.

“Legal services” will be provided in accordance with the terms and conditions set forth in this Coverage Part and will be provided by an attorney selected by the “insured organization” in consultation with “us”, from the list of attorney’s “we” provide.

S. “Loss” means:
1. “Damages”;
2. “Claims Expenses”; 
3. “Cyber Extortion Loss”; 
4. “Data Protection Loss” 
5. “Crisis Management and Public Relations 
6. “Penalties”; 
7. “PCI Fines, Expenses and Costs”; and 
8. “Privacy Breach Response Services.”

T. “Malicious code” means any virus, Trojan horse, worm or any other similar software program, code or script intentionally designed to insert itself into computer memory or onto a computer disk and spread itself from one computer to another.

U. “Management control” means:
1. Owning, directly or indirectly, more than fifty percent (50%) of the outstanding securities, representing the present right to vote for the election of an entity’s directors, members of the board of managers, management committee members or persons serving in a functionally equivalent role for such an entity operating or organization outside of the United States; or
2. Having the right, pursuant to a written contract or the bylaws, charter, operating agreement or similar documents of an entity to elect, appoint or designate a majority of:
   a. The Board of Directors of a corporation;
   b. The Management Committee of a joint venture or partnership;
   c. The Management Board of a Limited Liability Company; or
   d. Persons serving in a functionally equivalent role for such an entity operating or organized outside of the United States.

V. “Media material” means any information in electronic form, including words, sounds, numbers, images, or graphics and shall include advertising, video, streaming content, web-casting, online forum, bulletin board 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”.

W. “Merchant Services agreement” means any agreement between an “insured” and a financial institution, credit/debit card processor or independent service operator enabling an “insured” to accept credit card, debit card, prepaid card, or other payment cards for payments or donations.

X. “Notification services” means:
1. Notification by first class mail or e-mail to United States or Canadian residents; and
2. Notification by first class mail or e-mail to individuals residing outside the United States or Canada, but only to the extent reasonably practicable.

“Notification services” will be provided by a service provider selected by “us” in consultation with the “insured organization” from the list of service providers "we” provide and will be provided in accordance with the terms and conditions set forth in SECTION XI – CONDITIONS APPLICABLE TO PRIVACY BREACH RESPONSE SERVICES AND COVERAGE.

Y. “Notified individual” means an individual person to whom notice is given or attempted to be given under Paragraph 3. of SECTION I – B. Privacy Breach Response Services pursuant to a “breach notice law” as defined in Paragraph A. of SECTION X – DEFINITIONS.

Z. “PCI Fines, Expenses and Costs” means the direct monetary fines, penalties, reimbursements, fraud recoveries or assessments owed by the “insured organization” under the terms of a “merchant services agreement”, but only where such fines, penalties, reimbursements, fraud recoveries or assessments result both from the “insured organization’s” actual or alleged noncompliance with published Payment Card Industry (PCI) Data Security Standards and from a data breach caused by an incident (or reasonably suspected incident) described in
Paragraphs 1. and 2. of SECTION I – A. Information Security And Privacy Liability: provided, that the term “PCI Fines, Expenses and Costs” shall not include, or mean any charge backs, interchangeable fees, discount fees or prospective service fees.

AA. “Penalties” means:
1. Any civil fine or punitive sum of money payable to a governmental entity that was imposed in a “regulatory proceeding” by the Federal Trade Commission, Federal Communications Commission, or any other federal, state, local or foreign governmental entity, in such entity's regulatory or official capacity; the insurability of “penalties” shall be in accordance with the law in the applicable venue that most favors coverage for such “penalties”; and
2. Amounts which the “insured” is legally obligated to deposit in a fund as equitable relief for the payment of consumer claims due to an adverse judgment or settlement of a “regulatory proceeding”; but shall not include payments to charitable organizations or disposition of such funds other than for payment of consumer claims for losses caused by an event covered pursuant to Paragraphs 1., 2., or 3. of SECTION I – A. Information Security And Privacy Liability;

“Penalties” does not mean:
1. Costs to remediate or improve “computer systems”;
2. Costs to establish, implement, maintain, improve or remediate security or privacy practices, procedures, programs or policies;
3. Audit, assessment, compliance or reporting costs; or
4. Costs to protect the confidentiality, integrity and/or security of “personally identifiable information” from theft, loss or disclosure.

BB. “Personally identifiable information” means:
1. Information concerning the individual that constitutes nonpublic personal information as defined in the Gramm-Leach Bliley Act of 1999, as amended, and regulations issued pursuant the Act;
2. Medical or health care information concerning the individual, including protected health information as defined in the Health Insurance Portability and Accountability Act of 1996, as amended, and regulations issued pursuant to the Act.
3. Information concerning the individual that is defined as private personal information under statutes enacted to protect such information in foreign countries, for “claims’ subject to the law of such jurisdiction;
4. Information concerning the individual that is defined as private personal information under a “breach notice law”;
5. Education records as defined by the Family Educational Rights and Privacy Act (FERPA), which are directly related to an individual's attendance as a student; or
6. The individual's drivers license or state identification number, social security number, unpublished telephone number, and credit, debit, or other financial account numbers in combination with associated security codes, access codes, passwords or pins;

If such information allows an individual to be uniquely and reliably identified or contacted? or allows access to the individual's financial account or medial record information.

“Personally identifiable information” does not include publicly available information that is lawfully made available to the general public from government records.

CC. “Policy period” means the period of time between the inception date shown in the “declarations” and the effective date of termination, expiration or cancellation of this “insurance” the specifically excludes any “optional extension period” or any prior policy period or renewal period.

DD. “Privacy law” means a federal, state or foreign statute or regulation requiring the “insured organization” to protect the confidentiality and/or security of “personally identifiable information”.

EE. “Privacy policy” means the “insured organization's” public declaration of its policy for collection, use, disclosure, sharing, dissemination and correction or supplementation of, and access to “personally identifiable information”.

FF. “Public relations and crisis management expense” shall mean the follows costs approved in advance by “us”, and which are directly related to mitigating harm to the “insured organization’s” reputation or potential “loss” covered by this Coverage Part resulting from an incident described in Paragraphs 1. and 2. of SECTION I – A. Information Security And Privacy Liability or from a “public relations event”
1. Costs incurred by a public relations or crisis management consultant;
2. Costs for media purchasing or for printing or mailing materials intended to inform the general public about the incident, such costs to be limited to the amount noted in the Declarations for SECTION I – B. Privacy Breach Response Services;
3. For incidents or events in which notifications services are not otherwise provided pursuant to SECTION I – A. Information Security And Privacy Liability and B. Privacy Breach Response Services, costs to provide notifications and notices via e-mail or first class mail to customers or patient where such notifications are not required by law (voluntary notifications), including non-affected customers or patients of the “insured organization”;

RCG 2204 (0216)
4. Costs to provide government mandated public notices related to breach events (including such notifications required under HIPAA/Health Information Technology for Economic and Clinical Health Act ("HITECH")
5. Costs to provide services to restore healthcare records of "notified individuals" residing in the United States whose "personally identifiable information" was compromised as a result of theft, loss or "unauthorized disclosure".

"Public relations and crisis management expenses" must be incurred no later than twelve (12) months following the reporting of such "claim" or breach event to "us" and, with respect to Paragraphs 1. and 2. above, within ninety (90) days following the first publication of such "claim" or incident. If voluntary notifications are provided, e-mail notification will be provided in lieu of first class mail to the extent practicable.

GG. “Public relations event" means the publication or imminent publication in a newspaper (or other general circulation print publication) or on radio, television or a publically accessible website of a covered "claim" under this Coverage Part.

HH. "Regulatory proceeding" means a request for information, civil investigative demand or civil proceeding commenced by service of a compliant or similar proceeding brought by or on behalf of the Federal Trade Commission, Federal Communications Commission, or any federal, state, local or foreign governmental entity in such entity's regulatory or official capacity in connection with such proceeding.

II. "Related party" means the "insured organization" and any past, present or future employees, directors, officers, "managers", partners or natural person independent contractors of the "insured organization".

JJ. "Security breach" means:
1. "Unauthorized access or use of computer systems", including "unauthorized access or use" resulting from the theft of a password from a "computer system" or from any "insured";
2. A denial or service attack against "computer systems" or computer systems that are not owned, operated or controlled by an "insured"; or
3. Infection of "computer systems" by malicious code or transmission of malicious code from "computer systems".

A series of continuing “security breaches", related or repeated “security breaches", or multiple “security breaches" resulting from a continuing failure of "computer security" shall be considered a single “security breach" and be deemed to have occurred at the time of the first such “security breach".

KK. "Third party information" means any trade secret, data, design, interpretation, crop data, forecast, formula, method, practice, credit or debit card magnetic strip information, process, record, report or other item of information of a third party not insured under this Coverage Part which is not available to the general public and is provided to the "insured" subject to a mutually executed written confidentiality agreement or which the "insured organization" is legally required to maintain in confidence; however, "third party information" shall not include "personally identifiable information".

LL. "Unauthorized access or use" means the gaining of access to or use of "computer systems" by an unauthorized person or persons or the use of "computer systems" in an unauthorized manner.

MM. "Unauthorized disclosure" means the disclosure of (including disclosure resulting from phishing) or access to information in a manner that is not authorized by the "insured organization" and is without knowledge of, consent, or acquiescence of any member of the "control group".

SECTION XI – CONDITIONS APPLICABLE TO PRIVACY BREACH RESPONSE SERVICES AND COVERAGE

A. Insuring Agreements A., C., D., and G. only apply if:
1. The "insured organization" initiates the "notification services" described in Paragraph 3. SECTION I – B Privacy Breach Response Services as soon as practicable after the "insured's" discovery of the "claim";
2. The "claim" is made against the "insured" no later than two years after the "insured organization" initiates the notification services described in Paragraph 3 SECTION I.B. – Privacy Breach Response Services; and
3. The "insured" reports the "claim" to "us" in writing as soon as practicable.

B. The availability of any coverage under SECTION I – INSURING AGREEMENTS, B. Privacy Breach Response Services is subject to the following conditions.
1. We shall provide the "insured" with a list of the approved providers of "privacy breach response services" along with additional information about the Privacy Breach Response Services provided under this Coverage Part, and this information may be updated from time to time.
2. In the event that external forensics assistance is needed to assess the impact of a data incident on your computer system, the "computer security expert" will (1) help to determine whether, and the extent to
which, notification must be provided to comply with “breach notice laws” and (2) if applicable, give advice and oversight in connection with the investigation conducted by a PCI Forensic Investigator. The “computer security expert” will require access to information, files and systems and you must comply with the expert’s requests and cooperate with the expert’s investigation. Reports or findings of the expert will be made available to “you”, “us” and any attorney that is retained to provide advice to “you” with regard to the Incident.

3. If “legal services” are covered under SECTION I – INSURING AGREEMENTS, B. Privacy Breach Response Services the Beazley Breach Response Services team shall arrange “legal services” for “you”. The attorney will represent you in determining the applicability of, and the actions necessary to comply with, “breach notice laws” in connection with the Incident and to advise regarding credit card system operating regulation requirements, if applicable.

4. If “notification services” in connection with an Incident are covered, then Beazley Breach Response Services will assist “you” with the notification process, but it is important that “you” timely respond to requests, approve letter drafts, and provide address lists and other information as required to provide the “privacy breach response services”.

SECTION XII – PROOF AND APPRAISAL OF LOSS

A. Proof of Loss. With respect to Section I – G – Data Protection Loss, before coverage will apply, the Named Insured must:

1. prepare and submit to “us” a written and detailed proof of loss sworn by an officer of the Named Insured within ninety (90) days after the “insured” discovers a “data protection loss”, but in no event later than six (6) months following the end of the “policy period” (unless such period has been extended by “our” written consent). Such proof of loss shall include a narrative with full particulars of such “data protection loss”, including, the time, place and cause of the “data protection loss”, a detailed calculation of any “data protection loss”, the “insured organization’s” interest and the interest of all others in the property, the sound value thereof and the amount of “data protection loss” or damage thereto and all other insurance thereon; and

2. upon “our” request, submit to an examination under oath and provide copies of the underlying documents, data and materials that reasonably relate to or are part of the basis of the claim for such “data protection loss”.

The costs and expenses of preparing and submitting a proof of loss, and establishing or proving “data protection loss” or any other “loss” under this insurance shall be the “insured’s” obligation, and are not covered under this insurance.

B. Appraisal of Loss. If “we” do not agree with the “named insured” on the amount of a “loss”, each party shall select and pay an appraiser or other qualified expert (the “Appraiser”) to state the amount of the loss or reasonable expenses, and the Appraisers shall choose an umpire. If the Appraisers cannot agree on an umpire, the “named insured” or “we” may request a judge of a court having jurisdiction to make the selection. Each Appraiser shall submit the amount of the “loss” or reasonable expenses to the umpire, and agreement by the umpire and at least one of the Appraisers as to the amount of a “loss” shall be binding on all Insureds and “us”. The “named insured” and “we” will equally share the costs of the umpire and any other costs other than the cost of the Appraisers. This provision shall govern only the appraisal of the amount of a “loss”, and shall not control the determination of whether such “loss” is otherwise covered by this insurance. “We” will still retain and do not waive their rights to deny coverage or enforce any obligation under this insurance.

SECTION XIII – RECOVERED PROPERTY

If the “insured” or “we” recover any property, money or “data assets” after a loss payment is made, the party making the recovery must give prompt notice of the recovery to the other party. If the recovered property is money or other funds, the recovery shall be applied first to any costs incurred by “us” in recovering the property, second to loss payments made by “us”, and third to any “retention” payment made by the “named insured”. If property other than money or funds is recovered, then the “named insured” may keep the recovered property and return the loss payment, plus any costs of recovery incurred by “us”, or keep the loss payment less the costs of recovery incurred by “us” and transfer all rights in the property to “us”.

SECTION XIV – OBLIGATIONS IN THE EVENT OF AN EXTORTION THREAT

A. Insured’s Duty of Confidentiality
The “insured” shall use its best efforts at all times to ensure that knowledge regarding the existence of this insurance for “cyber extortion loss” afforded by this insurance is kept confidential. “We” may terminate the insurance provided by this policy for “cyber extortion loss” upon ten (10) days written notice to the “named insured” if the existence of insurance for “cyber extortion loss” provided by this insurance becomes public knowledge or is revealed to a person making an “extortion threat” through no fault of “ours”.

B. Insured Organization’s Obligation to Investigate Extortion Threat and Avoid or Limit Extortion Payment
Prior to the payment of any “extortion payment”, the “insured” shall make every reasonable effort to determine that the “extortion threat” is not a hoax, or otherwise not credible. The “insured” shall take all steps reasonable and practical to avoid or limit the payment of an “extortion payment”.

C. Conditions Precedent
As conditions precedent to this insurance for “cyber extortion loss” under the terms of this insurance:

1. **Named Insured’s Obligation to Demonstrate Duress**
   The “insured” must be able to demonstrate that the “extortion payment” was surrendered under duress.

2. **Notification of Police**
   The “insured” shall allow “us” or their representative to notify the police or other responsible law enforcement authorities of any “extortion threat”.
