

---

# HSB Total Cyber™

## Cyber Risk Coverage Part Declarations

---

### Producer Information

Name and Mailing Address

### Insuring Company

Name The Hartford Steam Boiler Inspection and Insurance Company  
Mailing Address One State Street, Hartford, Connecticut 06102-5024  
Contact Information:  
*To report a claim* Phone: 1-888-HSB-LOSS (472-5677)  
Fax: 1-888-329-5677  
Email: [New\\_Loss@hsb.com](mailto:New_Loss@hsb.com)

*To ask a question or  
request a change to  
your policy*

Phone: 1-800-472-1866

### Policy Information

Named Insured Sample Policy  
Headquarters Address 123 Sample St, Hartford, CT 06105  
Mailing Address Same as above  
Policy Number TBD  
Reason for Issuance New Business  
Issue Date 09/17/2021  
Transaction Effective Date 10/01/2021  
Retroactive Date If no retroactive date is shown, retroactive date is the organization date of the Named Insured.

### Policy Period

Policy Period 10/01/2021 to 10/01/2022  
Effective at 12:01 A.M. Standard Time at your mailing address shown above.

### Transaction Premium Summary

Cyber Risk Coverage	\$356.00
Terrorism	\$0

### Limit

#### Cyber Risk Aggregate Limit

Cyber Risk Aggregate Limit	\$100,000
----------------------------	-----------

### Coverage

#### Coverage

#### Amount

<b>1.</b>	<b>Data Compromise Response Expenses</b> (Annual Aggregate Limit)	\$100,000
	Crisis Management Sublimit (Any one "Personal Data Compromise")	\$100,000
	Regulatory Fines and Penalties Sublimit (Any one "Personal Data Compromise")	\$100,000
	PCI Fines and Penalties Sublimit (Any one "Personal Data Compromise")	\$100,000
	PCI Assessments	Included
	Additional Response Expenses Limit	Not Covered
	Deductible (Any one "Personal Data Compromise")	\$2,500
<b>2.</b>	<b>Identity Recovery</b> Annual Aggregate Limit	\$25,000
	Lost Wages and Child and Elder Care Sublimit	\$5,000
	Mental Health Counseling Sublimit	\$5,000
	Miscellaneous Unnamed Costs Sublimit	\$1,000
	Deductible	Not Applicable

Identity Recovery Help Line Number: 1-800-472-1866

<u>Coverage</u>	<u>Amount</u>
<b>3. Computer Attack</b> (Annual Aggregate Limit)	\$100,000
Data Re-creation Sublimit (Any one "Computer Attack")	\$100,000
Crisis Management Sublimit (Any one "Computer Attack")	\$100,000
Future Loss Avoidance	Not Covered
Deductible (Any one "Computer Attack")	\$2,500
<b>Loss of Business Sublimit</b> (Including Extended Income Recovery) (Any one "Computer Attack")	\$100,000
Contingent Loss of Business (Any one "Computer Attack")	\$100,000
"Waiting Period"	8 Hours
"Maximum Period of Restoration"	180 Days
"Extended Recovery Period"	30 Days
Costs of Forensic Accountant	Included
<b>Contingent Loss of Business – Interruption of Supply Sublimit</b> (Any one "Computer Attack")	Not Covered
<b>4. Cyber Extortion</b> (Annual Aggregate Limit)	\$100,000
Deductible (Any one "Cyber Extortion Threat")	\$2,500
<b>5. Data Compromise Liability</b> (Annual Aggregate Limit)	\$100,000
Data Compromise Defense	Included
Data Compromise Liability	Included
Privacy Incident Liability	Not Covered
Deductible (Any one "Claim" or "Regulatory Proceeding")	\$2,500
<b>6. Network Security Liability</b> (Annual Aggregate Limit)	\$100,000
Network Security Defense	Included
Network Security Liability	Included
Deductible (Any one "Claim")	\$2,500
<b>7. Electronic Media Liability</b> (Annual Aggregate Limit)	\$100,000
Electronic Media Defense	Included
Electronic Media Liability	Included
Full Media Liability	Included
Deductible (Any one "Claim")	\$2,500

<u>Coverage</u>	<u>Amount</u>
<b>8. Misdirected Payment Fraud</b> (Annual Aggregate Limit)	\$100,000
Computer Fraud Sublimit (Any one "Computer Fraud Event")	\$100,000
Invoice Manipulation Fraud Sublimit (Any one "Invoice Manipulation Fraud Event")	\$100,000
Deductible (Any one "Wrongful Transfer Event", "Computer Fraud Event" or "Invoice Manipulation Fraud Event")	\$2,500
<b>Business Identity Theft</b> (Annual Aggregate Limit)	\$100,000
Business Identity Theft Defense	Included
Business Identity Theft Liability	Included
Deductible (Any one "Claim" or "Regulatory Proceeding")	\$2,500
<b>Cryptojacking</b> (Annual Aggregate Limit)	\$100,000
Deductible (Any one "Cryptojacking Event")	\$2,500
<b>Reputational Harm</b> (Annual Aggregate Limit)	\$100,000
"Period of Indemnification"	30 Days
Deductible (Any one "Personal Data Compromise")	\$2,500
<b>Reward Payment Reimbursement</b> (Annual Aggregate Limit)	\$50,000
Deductible (Any one "Reward Payment Qualifying Event")	\$2,500
<b>System Failure</b> (Annual Aggregate Limit)	Not Covered
Contingent System Failure (Any one "System Failure")	Not Covered
Deductible (Any one "System Failure")	Not Covered
<b>Telecommunications Fraud</b> (Annual Aggregate Limit)	\$100,000
Deductible (Any one "Computer Attack")	\$2,500

## Forms

*This policy is made up of this Cyber Risk Coverage Part Declarations and the following forms:*

<u>Form Name</u>	<u>Form Number</u>	<u>Eff. Date</u>	<u>Issue Date</u>
Agreement and Conditions	AC 200 01 2021	10/01/2021	09/17/2021
HSB Total Cyber Cyber Risk Coverage Form	HTC 201 01 2017	10/01/2021	09/17/2021
Additional Insured - Pursuant To A Contract	HTC AICON 03 2020	10/01/2021	09/17/2021
Business Identity Theft Liability	HTC BIT 01 2021	10/01/2021	09/17/2021
Cost of Forensic Accountant	HTC CFA 03 2020	10/01/2021	09/17/2021
Cryptojacking	HTC CRYPTO 01 2021	10/01/2021	09/17/2021
Extended Income Recovery	HTC EIR 03 2020	10/01/2021	09/17/2021
Full Media Liability	HTC FML 03 2020	10/01/2021	09/17/2021
HSB Total Cyber Enhancement Endorsement	HTC ENH 01 2021	10/01/2021	09/17/2021
Invoice Manipulation Fraud	HTC IM 01 2021	10/01/2021	09/17/2021
PCI Assessments, Fines and Penalties	HTC PCIFP 03 2020	10/01/2021	09/17/2021
Reputational Harm	HTC RH 03 2020	10/01/2021	09/17/2021
Telecommunications Fraud	HTC TF 03 2020	10/01/2021	09/17/2021
Terrorism Risk Insurance Act Disclosure	HTC TRIA 07 20 )	10/01/2021	09/17/2021

Sample

## Agreement and Conditions

### The Hartford Steam Boiler Inspection and Insurance Company

One State Street  
Hartford, Connecticut 06102-5024

(A Stock Insurance Company)

### Insuring Agreement

In return for payment of the premium and subject to the terms of this policy, we agree with you to provide the insurance as stated in this policy.

In Witness Whereof, the Company identified on the Declarations has caused this policy to be signed by its President and Corporate Secretary at Hartford, Connecticut.



Greg Barats  
President and Chief Executive Officer



Nancy C. Onken  
Corporate Secretary

# General Conditions

## I. COMMON POLICY CONDITIONS

### A. CANCELLATION

1. The first Named Insured shown in the Declarations may cancel this policy by mailing or delivering to us advance written notice of cancellation.
2. We may cancel this policy by mailing or delivering to the first Named Insured written notice of cancellation at least:
  - a. 10 days before the effective date of cancellation if we cancel for nonpayment of premium; or
  - b. 30 days before the effective date of cancellation if we cancel for any other reason.
3. We will mail or deliver our notice to the first Named Insured's last mailing address known to us.
4. Notice of cancellation will state the effective date of cancellation. The policy period will end on that date.
5. If this policy is canceled, we will send the first Named Insured any premium refund due. If we cancel, the refund will be pro rata. 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.
6. If notice is mailed, proof of mailing will be sufficient proof of notice.

### B. 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 consent. This policy's terms can be amended or waived only by endorsement issued by us and made a part of this policy.

### C. 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 and up to three years afterward.

### D. INSPECTIONS AND SURVEYS

1. We have the right to:
  - a. Make inspections and surveys at any time;
  - b. Give you reports on the conditions we find; and
  - c. Recommend changes.
2. We are not obligated to make any inspections, surveys, reports or recommendations and any such actions 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:
  - a. Are safe or healthful; or
  - b. Comply with laws, regulations, codes or standards.
3. Paragraphs 1. and 2. of this condition apply not only to us, but also to any rating, advisory, rate service or similar organization which makes insurance inspections, surveys, reports or recommendations.

### E. PREMIUMS

The first Named Insured shown in the Declarations:

1. Is responsible for the payment of all premiums; and
2. Will be the payee for any return premiums we pay.

### F. 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 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.

**G. TITLES OF PARAGRAPHS**

Titles given to paragraphs throughout this policy are for assistance in finding applicable provisions. Titles do not grant, define or restrict coverage.

**II. CALCULATION OF PREMIUM**

The premium shown in the Declarations was computed based on rates in effect at the time the policy was issued. On each renewal, continuation, or anniversary of the effective date of this policy, we will compute the premium in accordance with our rates and rules then in effect.

**III. REPORT OF VALUES**

You must report exposure information to us at least once a year.

**IV. ADJUSTMENT OF PREMIUM**

- A. The premium charged at the inception of each policy year is an advance premium. When we receive updated exposure information from you or when we determine updated exposure information through an audit or claim adjustment, we will determine an adjusted premium for this insurance.
- B. If the adjusted premium is less than the advance premium, we will return the excess premium to you. Such excess premium will not exceed 75% of the advance premium.
- C. If the adjusted premium is greater than the advance premium, we will charge the additional premium based on your reports of value.

Sample



# HSB Total Cyber™

## Cyber Risk Coverage Form

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.

Other words and phrases that appear in quotation marks have special meaning. Refer to section H. DEFINITIONS.

### A. COVERAGE

This section lists the coverages that may apply if indicated in the Declarations. Each coverage is subject to a specific aggregate limit as shown in the Declarations. See paragraph C.2. for details.

#### 1. Data Compromise Response Expenses

- a. Coverage 1 – Data Compromise Response Expenses applies only if all of the following conditions are met:
- (1) There has been a “personal data compromise”; and
  - (2) Such “personal data compromise” took place in the “coverage territory”; and
  - (3) Such “personal data compromise” is first discovered by you during the “coverage term”; and
  - (4) Such “personal data compromise” is reported to us within 60 days after the date it is first discovered by you.
- b. If the conditions stated in a. above have been met, then we will provide coverage for the following expenses when they arise directly from the “personal data compromise” described in a. above and are necessary and reasonable. Items (4) and (5) below apply only if there has been a notification of the “personal data compromise” to “affected individuals” as covered under item (3) below.

##### (1) Forensic IT Review

Professional information technologies review if needed to determine, within the constraints of what is possible and reasonable, the nature and extent of the “personal data compromise” and the number and identities of the “affected individuals”.

This does not include costs to analyze, research or determine any of the following:

- (a) Vulnerabilities in systems, procedures or physical security;
- (b) Compliance with Payment Card Industry or other industry security standards; or
- (c) The nature or extent of loss or damage to data that is not “personally identifying information” or “personally sensitive information”.

If there is reasonable cause to suspect that a covered “personal data compromise” may have occurred, we will pay for costs covered under Forensic IT Review, even if it is eventually determined that there was no covered “personal data compromise”. However, once it is determined that there was no covered “personal data compromise”, we will not pay for any further costs.

##### (2) Legal Review

Professional legal counsel review of the “personal data compromise” and how you should best respond to it.

If there is reasonable cause to suspect that a covered “personal data compromise” may have occurred, we will pay for costs covered under Legal Review, even if it is eventually determined that there was no covered “personal data compromise”. However, once it is determined that there was no covered “personal data compromise”, we will not pay for any further costs.

##### (3) Notification to Affected Individuals

We will pay your necessary and reasonable costs to provide notification of the “personal data

compromise” to “affected individuals”.

**(4) Services to Affected Individuals**

We will pay your necessary and reasonable costs to provide the following services to “affected individuals”. Services (c) and (d) below apply only to “affected individuals” from “personal data compromise” events involving “personally identifying information”.

**(a) Informational Materials**

A packet of loss prevention and customer support information.

**(b) Help Line**

A toll-free telephone line for “affected individuals” with questions about the “personal data compromise”. Where applicable, the line can also be used to request additional services as listed in (c) and (d) below.

**(c) Credit Report and Monitoring**

A credit report and an electronic service automatically monitoring for activities affecting an individual’s credit records. This service is subject to the “affected individual” enrolling for this service with the designated service provider.

**(d) Identity Restoration Case Management**

As respects any “affected individual” who is or appears to be a victim of “identity theft” that may reasonably have arisen from the “personal data compromise”, the services of an identity restoration professional who will assist that “affected individual” through the process of correcting credit and other records and, within the constraints of what is possible and reasonable, restoring control over his or her personal identity.

**(5) Crisis Management**

Professional public relations firm review of and response to the potential impact of the “personal data compromise” on your business relationship.

This includes costs to implement public relations recommendations of such firm. This may include advertising and special promotions designed to reinvigorate your relationship with “affected individuals”. However, we will not pay for:

- (a) Promotions provided to any of your “executives” or “employees”; or
- (b) Promotion costs exceeding \$25 per “affected individual”.

**(6) Regulatory Fines and Penalties**

Any fine or penalty imposed by law, to the extent such fine or penalty is legally insurable under the law of the applicable jurisdiction.

**(7) PCI Fines and Penalties**

Any Payment Card Industry fine or penalty imposed under a contract to which you are a party. PCI Fines and Penalties do not include any increased transaction costs.

**2. Identity Recovery**

a. Coverage 2 – Identity Recovery applies only if all of the following conditions are met:

- (1) There has been an “identity theft” involving the personal identity of an “identity recovery insured” under this Coverage Part; and
- (2) Such “identity theft” took place in the “coverage territory”; and
- (3) Such “identity theft” is first discovered by the “identity recovery insured” during the “coverage term”; and
- (4) Such “identity theft” is reported to us within 60 days after it is first discovered by the “identity recovery insured”.

b. If the conditions listed in a. above have been met, then we will provide the following to the “identity recovery insured”:

**(1) Case Management Service**

Services of an “identity recovery case manager” as needed to respond to the “identity theft”;

and

**(2) Expense Reimbursement Coverage**

Reimbursement of necessary and reasonable “identity recovery expenses” incurred as a direct result of the “identity theft”.

**3. Computer Attack**

a. Coverage 3 – Computer Attack applies only if all of the following conditions are met:

- (1) There has been a “computer attack”; and
- (2) Such “computer attack” occurred in the “coverage territory”; and
- (3) Such “computer attack” is first discovered by you during the “coverage term”; and
- (4) Such “computer attack” is reported to us as soon as practicable, but in no event more than 60 days after the date it is first discovered by you.

b. If the conditions listed in a. above have been met, then we will provide you the following coverages for “loss” directly arising from such “computer attack”.

**(1) Data Restoration**

We will pay your necessary and reasonable “data restoration costs”.

**(2) Data Re-creation**

We will pay your necessary and reasonable “data re-creation costs”.

**(3) System Restoration**

We will pay your necessary and reasonable “system restoration costs”.

**(4) Loss of Business**

We will pay your actual “business income and extra expense loss” resulting from a “computer attack” on a “computer system” owned or leased by you and operated under your control.

**(5) Contingent Loss of Business**

We will pay your actual “business income and extra expense loss” resulting from a “computer attack” on a “computer system” operated by a third party service provider used for the purpose of providing hosted computer application services to you or for processing, maintaining, hosting or storing your electronic data, pursuant to a written contract with you for such services.

**(6) Crisis Management**

If you suffer a covered “business income and extra expense loss”, we will pay for the services of a professional public relations firm to assist you in communicating your response to the “computer attack” to the media, the public and your customers, clients or members.

**4. Cyber Extortion**

a. Coverage 4 – Cyber Extortion applies only if all of the following conditions are met:

- (1) There has been a “cyber extortion threat”; and
- (2) Such “cyber extortion threat” is first made against you during the “coverage term”; and
- (3) Such “cyber extortion threat” is reported to us as soon as practicable, but in no event more than 60 days after the date it is first made against you.

b. If the conditions listed in a. above have been met, then we will pay the “cyber extortion expenses” that result from such “cyber extortion threat”.

c. You must make every reasonable effort not to divulge the existence of this coverage.

**5. Data Compromise Liability**

a. Coverage 5 – Data Compromise Liability applies only if all of the following conditions are met:

- (1) During the “coverage term” or any applicable Extended Reporting Period, you first receive notice of one of the following:
  - (a) A “claim”; or;

- (b) A “regulatory proceeding” brought by a governmental entity.
- (2) Such “claim” or “regulatory proceeding” must arise from a “personal data compromise” that:
  - (a) Took place on or after the Retroactive Date, if any, shown in the Declarations and before the end of the “policy period”;
  - (b) Took place in the “coverage territory”; and
  - (c) Was submitted to us and insured under Coverage 1 – Data Compromise Response Expenses.
- (3) Such “claim” is reported to us as soon as practicable, but in no event more than 60 days after the date it is first received by you.
- b. If the conditions listed in a. above have been met, then we will pay on behalf of the “insured”:
  - (1) “Loss” directly arising from the “claim”; or
  - (2) “Defense costs” directly arising from a “regulatory proceeding”.
- c. All “claims” and “regulatory proceedings” arising from a single “personal data compromise” or “interrelated” “personal data compromises” will be deemed to have been made at the time that notice of the first of those “claims” or “regulatory proceedings” is received by you.

## 6. Network Security Liability

- a. Coverage 6 – Network Security Liability applies only if all of the following conditions are met:
  - (1) During the “coverage term” or any applicable Extended Reporting Period, you first receive notice of a “claim” which arises from a “network security incident” that:
    - (a) Took place on or after the Retroactive Date, if any, shown in the Declarations and before the end of the “policy period”; and
    - (b) Took place in the “coverage territory”; and
  - (2) Such “claim” is reported to us as soon as practicable, but in no event more than 60 days after the date it is first received by you.
- b. If the conditions listed in a. above have been met, then we will pay on behalf of the “insured” “loss” directly arising from the “claim”.
- c. All “claims” arising from a single “network security incident” or “interrelated” “network security incidents” will be deemed to have been made at the time that notice of the first of those “claims” is received by you.

## 7. Electronic Media Liability

- a. Coverage 7 – Electronic Media Liability applies only if all of the following conditions are met:
  - (1) During the “coverage term” or any applicable Extended Reporting Period, you first receive notice of a “claim” which arises from an “electronic media incident” that:
    - (a) Took place on or after the Retroactive Date, if any, shown in the Declarations and before the end of the “policy period”; and
    - (b) Took place in the “coverage territory”; and
  - (2) Such “claim” is reported to us as soon as practicable, but in no event more than 60 days after the date it is first received by you.
- b. If the conditions listed in a. above have been met, then we will pay on behalf of the “insured” “loss” directly arising from the “claim”.
- c. All “claims” arising from a single “electronic media incident” or “interrelated” “electronic media incidents” will be deemed to have been made at the time that notice of the first of those “claims” is received by you.

## 8. Misdirected Payment Fraud

- a. This Misdirected Payment Fraud coverage applies only if all of the following conditions are met:
  - (1) There has been a “wrongful transfer event” against you;
  - (2) Such “wrongful transfer event” took place in the “coverage territory”;

- (3) Such “wrongful transfer event” is first discovered by you during the “coverage term”;
  - (4) Such “wrongful transfer event” is reported to us within 60 days after the date it is first discovered by you; and
  - (5) Such “wrongful transfer event” is reported in writing by you to the police.
- b. If the conditions listed above in a. have been met, then we will pay your necessary and reasonable “wrongful transfer costs” arising directly from the “wrongful transfer event”.

## B. EXCLUSIONS

### 1. General Exclusions

The following exclusions are applicable to all coverage sections.

This insurance does not apply to “loss” or “claims” based upon, attributable to or arising out of:

#### a. Nuclear

Nuclear reaction or radiation or radioactive contamination, however caused.

#### b. War

War and military action including any of the following and any consequence of any of the following:

- (1) War, including undeclared or civil war;
- (2) Warlike action by military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents; or
- (3) Insurrection, rebellion, revolution, usurped power, political violence or action taken by governmental authority in hindering or defending against any of these.

### 2. General Exclusions Not Applicable to Coverage 2 – Identity Recovery

The following exclusions are applicable to all coverage sections except for Coverage 2 – Identity Recovery.

This insurance does not apply to “loss” or “claims” based upon, attributable to or arising out of:

#### a. Contractual Liability

Any liability arising out of any actual or alleged contractual liability of any “insured” under any express contract or agreement. This exclusion, however, shall not apply to:

- (1) Any PCI Fines and Penalties covered under Coverage 1 – Data Compromise Response Expenses; or
- (2) Any liability the “insured” would have in the absence of such express contract or agreement.

#### b. Criminal Investigations or Proceedings

Any criminal investigations or proceedings.

However, this exclusion does not apply to “defense costs” arising from an otherwise insured “wrongful act”.

#### c. Deficiency Correction

Costs to research or correct any deficiency.

#### d. Fines and Penalties

Any fines or penalties other than those explicitly covered under Coverage 1 – Data Compromise Response Expenses.

#### e. Fraudulent, Dishonest or Criminal Acts

Any criminal, fraudulent or dishonest act, error or omission, or any intentional or knowing violation of the law by the “insured”.

#### f. Government Organizations

Any liability arising from “claim(s)” against you brought by or on behalf of any federal, state or local government agency or professional or trade licensing organizations; however, this exclusion shall not apply to:

- (1) Actions or proceedings brought by a governmental authority or regulatory agency acting solely in its capacity as a customer of the “named insured” or a “subsidiary”; or
- (2) “Regulatory proceedings” insured under Coverage 5 – Data Compromise Liability.

**g. Information Technology Products**

The propagation or forwarding of malware, including viruses, worms, Trojans, spyware and keyloggers in connection with hardware or software created, produced or modified by you for sale, lease or license to third parties.

**h. Infrastructure Failure**

Failure or interruption of or damage to any electrical power supply network or telecommunication network not owned and operated by the insured including, but not limited to, the internet, internet service providers, Domain Name System (DNS) service providers, cable and wireless providers, internet exchange providers, search engine providers, internet protocol networks (and similar networks that may have different designations) and other providers of telecommunications or internet infrastructure.

**i. Knowledge of Falsity**

Any oral or written publication of material, if done by the “insured” or at the “insured’s” direction with knowledge of its falsity.

**j. Non-monetary Relief**

That part of any “claim” seeking any non-monetary relief.

However, this exclusion does not apply to “defense costs” arising from an otherwise insured “wrongful act”.

**k. Pollution**

Any liability arising out of the presence of or the actual, alleged or threatened discharge, dispersal, release or escape of “pollutants”, or any direction or request to test for, monitor, clean up, remove, contain, treat, detoxify or neutralize “pollutants”, or in any way respond to or assess the effects of “pollutants”.

**l. Prior Notice**

The same facts, “wrongful acts” 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 Coverage Part is a renewal or replacement or which it may succeed in time.

**m. Prior Knowledge**

Any incident, circumstance or “wrongful act” which an “insured”:

- (1) Had knowledge of; or
- (2) Could reasonably have foreseen might result in a “claim”;

and which was known to the “insured” prior to the earlier of the effective date of this Coverage Part or the first Coverage Part issued by us of which this Coverage Part is an uninterrupted renewal.

**n. Prior Wrongful Acts**

Any “wrongful act” first occurring before the Retroactive Date, if any, shown in the Declarations.

**o. Prior or Pending Litigation**

Any “claim”, “regulatory proceeding” or other proceeding against an “insured” which was pending or existed prior to the earlier of the following dates:

- (1) The inception of this Coverage Part; or
- (2) The inception of the original Coverage Part of which this Coverage Part is a renewal or replacement;

or arising out of the same or substantially the same facts, circumstances or allegations which are the subject of, or the basis for, such “claim”, “regulatory proceeding” or other proceeding.

**p. Property Damage or Bodily Injury**

“Property damage” or “bodily injury” other than mental anguish or mental injury alleged in a “claim” covered under Coverage 7 – Electronic Media Liability.

**q. Reckless Disregard**

Your reckless disregard for the security of “personally identifying information”, “personally sensitive information” or “third party corporate data” in your care, custody or control.

**r. Uninsurable by Law**

Any amount not insurable under applicable law.

**s. Willful Complicity**

The “insured’s” intentional or willful complicity in a covered “claim” or “loss” event, or your reckless disregard for the security of your “computer system” or data.

**3. Additional Exclusions Applicable to Coverage 2 – Identity Recovery**

The following additional exclusions are applicable to Coverage 2 – Identity Recovery.

This insurance does not apply to:

**a. Fraudulent, Dishonest or Criminal Acts**

Any fraudulent, dishonest or criminal act by an “identity recovery insured” or any person aiding or abetting an “identity recovery insured”, or by any “authorized representative” of an “identity recovery insured”, whether acting alone or in collusion with others. However, this exclusion will not apply to the interests of an “identity recovery insured” who has no knowledge of or involvement in such fraud, dishonesty or criminal act.

**b. Professional or Business Identity**

The theft of a professional or business identity.

**c. Unreported Identity Theft**

An “identity theft” that is not reported in writing to the police.

**4. Additional Exclusion Applicable to Coverage 3 – Computer Attack**

The following additional exclusion is applicable to Coverage 3 – Computer Attack.

This insurance does not apply to:

**Computers of Others**

Failure or interruption of or damage (including, but not limited to, damage to data, software and operating systems) to a computer or other electronic hardware that is not a “computer system”.

**C. LIMITS OF INSURANCE**

Any payment made under this Coverage Part will not be increased if more than one insured is shown in the Declarations or if you are comprised of more than one legal entity. Note that the limits described below apply to “defense costs” as well as other covered “loss”. See the definition of “loss”. Note also that post-judgment interest is covered outside of the coverage limits as described in section E.4.

**1. Cyber Risk Aggregate Limit**

The Cyber Risk Aggregate Limit shown in the Declarations is the most we will pay for all “loss” under all applicable coverage sections in any one “coverage term” or any applicable Extended Reporting Period. The Cyber Risk Aggregate Limit shown in the Declarations applies regardless of the number of insured events first discovered or “claims” or “regulatory proceedings” first received during the “coverage term” or any applicable Extended Reporting Period.

**2. Coverage Aggregate Limits**

The aggregate limit for each coverage section shown in the Declarations is the most we will pay for all “loss” under that coverage section in any one “coverage term” or any applicable Extended Reporting Period. The aggregate limit shown in the Declarations applies regardless of the number of insured events first discovered or “claims” or “regulatory proceedings” first received during the “coverage term” or any applicable Extended Reporting Period. The aggregate limit for each coverage section is part of, and not in addition to, the Cyber Risk Aggregate Limit.

**3. Coverage Sublimits**

**a. Coverage 1 Sublimits**

The most we will pay under Coverage 1 – Data Compromise Response Expenses for Crisis Management, Regulatory Fines and Penalties and PCI Fines and Penalties coverages for “loss” arising from any one “personal data compromise” is the applicable sublimit for each of those coverages shown in the Declarations. These sublimits are part of, and not in addition to, the aggregate limit for Coverage 1 shown in the Declarations. Crisis Management coverage is also subject to a limit per “affected individual” as described in A.1.b.(5).

**b. Coverage 2 Sublimits**

The following provisions are applicable to Coverage 2 – Identity Recovery.

- (1) Case Management Service is available as needed for any one “identity theft” for up to 12 consecutive months from the inception of the service. Expenses we incur to provide Case Management Services do not reduce the aggregate limit for Coverage 2 – Identity Recovery.
- (2) Costs covered under item d. (Legal Costs) of the definition of “identity recovery expenses” are part of, and not in addition to, the aggregate limit for Coverage 2 – Identity Recovery.
- (3) Costs covered under item e. (Lost Wages) and item f. (Child and Elder Care Expenses) of the definition of “identity recovery expenses” are jointly subject to the Lost Wages and Child and Elder Care sublimit shown in the Declarations. This sublimit is part of, and not in addition to, the aggregate limit for Coverage 2 – Identity Recovery. Coverage is limited to wages lost and expenses incurred within 12 months after the first discovery of the “identity theft” by the “identity recovery insured”.
- (4) Costs covered under item g. (Mental Health Counseling) of the definition of “identity recovery expenses” is subject to the Mental Health Counseling sublimit shown in the Declarations. This sublimit is part of, and not in addition to, the aggregate limit for Coverage 2 – Identity Recovery. Coverage is limited to counseling that takes place within 12 months after the first discovery of the “identity theft” by the “identity recovery insured”.
- (5) Costs covered under item h. (Miscellaneous Unreimbursed Costs) of the definition of “identity recovery expenses” is subject to the Miscellaneous Unreimbursed Costs sublimit shown in the Declarations. This sublimit is part of, and not in addition to, the aggregate limit for Coverage 2 – Identity Recovery. Coverage is limited to costs incurred within 12 months after the first discovery of the “identity theft” by the “identity recovery insured”.

**c. Coverage 3 Sublimits**

The most we will pay under Coverage 3 – Computer Attack for Data Re-Creation, Loss of Business and Crisis Management coverages for “loss” arising from any one “computer attack” is the applicable sublimit for each of those coverages shown in the Declarations. The most we will pay under Coverage 3 – Computer Attack for Contingent Loss of Business coverage for “loss” arising from any one “computer attack” is the Loss of Business sublimit shown in the Declarations. These sublimits are part of, and not in addition to, the aggregate limit for Coverage 3 – Computer Attack shown in the Declarations.

**4. Application of Limits**

- a. A “computer attack”, “cyber extortion threat”, “personal data compromise”, “identity theft” or “wrongful transfer event” may be first discovered by you in one “coverage term” but it may cause insured “loss” in one or more subsequent “coverage terms”. If so, all insured “loss” arising from such “computer attack”, “cyber extortion threat”, “personal data compromise”, “identity theft” or “wrongful transfer event” will be subject to the limit of insurance applicable to the “coverage term” when the “computer attack”, “cyber extortion threat”, “personal data compromise”, “identity theft” or “wrongful transfer event” was first discovered by you.
- b. You may first receive notice of a “claim” or “regulatory proceeding” in one “coverage term” but it may cause insured “loss” in one or more subsequent “coverage terms”. If so, all insured “loss” arising from such “claim” or “regulatory proceeding” will be subject to the limits of insurance applicable to the “coverage term” when notice of the “claim” or “regulatory proceeding” was first received by you.
- c. The limit of insurance for the Extended Reporting Periods (if applicable) will be part of, and not in addition to, the limit of insurance for the immediately preceding “coverage term”.



- d. Coverage for Services to Affected Individuals under Coverage 1 – Data Compromise Response Expenses is limited to costs to provide such services for a period of up to one year from the date of the notification to the “affected individuals”. Notwithstanding, coverage for Identity Restoration Case Management services initiated within such one year period may continue for a period of up to one year from the date such Identity Restoration Case Management services are initiated.

#### **D. DEDUCTIBLES**

1. We will not pay for “loss” under any coverage section until the amount of the insured “loss” exceeds the deductible amount shown in the Declarations for that coverage section. We will then pay the amount of “loss” in excess of the applicable deductible amount, subject to the applicable limits shown in the Declarations. You will be responsible for the applicable deductible amount.
2. The deductible will apply to all:
  - a. “Loss” arising from the same insured event or “interrelated” insured events under Coverage 1 – Data Compromise Response Expenses, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion or Coverage 8 – Misdirected Payment Fraud.
  - b. “Loss” resulting from the same “wrongful act” or “interrelated” “wrongful acts” insured under Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability or Coverage 7 – Electronic Media Liability.
3. In the event that “loss” is insured under more than one coverage section, only the single highest deductible applies.
4. Insurance coverage under Coverage 2 – Identity Recovery is not subject to a deductible.

#### **E. DEFENSE AND SETTLEMENT**

The following provisions are applicable to Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability, and Coverage 7 – Electronic Media Liability.

1. We will have the legal duty to defend and appoint an attorney to defend the “insured” against any “claim” or “regulatory proceeding” insured by this Coverage Part, regardless of whether the allegations of such “claim” or “regulatory proceeding” are groundless, false or fraudulent. However, we will have no duty to defend the “insured” against any claim or “regulatory proceeding” seeking damages or other relief not insured by this Coverage Part.

At the time a “claim” or “regulatory proceeding” is first reported to us, you may request that we appoint a defense attorney of your choice. We will give full consideration to any such request.
2. We may, with your written consent, make any settlement of a “claim” or “regulatory proceeding” which we deem reasonable. If you refuse to consent to any settlement recommended by us and acceptable to the claimant or plaintiff, our liability for all “loss” or “defense costs” resulting from such “claim” or “regulatory proceeding” will not exceed the amount for which we could have settled such “claim” or “regulatory proceeding” plus “defense costs” incurred as of the date we proposed such settlement in writing to you.
3. We will not be obligated to pay any “loss” or “defense costs”, or to defend or continue to defend any “claim” or “regulatory proceeding” after the applicable limit of insurance has been exhausted.
4. We will pay all interest on that amount of any judgment within the applicable limit of insurance which accrues:
  - a. After entry of judgment; and
  - b. Before we pay, offer to pay or deposit in court that part of the judgment within the applicable limit of insurance or, in any case, before we pay or offer to pay the entire applicable limit of insurance.

These interest payments will be in addition to and not part of the applicable limit of insurance.

#### **F. EXTENDED REPORTING PERIODS**

The following provisions are applicable to Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability, and Coverage 7 – Electronic Media Liability.

1. You will have the right to the Extended Reporting Periods described in this section, in the event of a “termination of coverage”.
2. If a “termination of coverage” has occurred, you will have the right to the following:
  - a. An Automatic Extended Reporting Period of 60 days after the effective date of the “termination of

coverage” at no additional premium in which to give to us written notice of a “claim” or “regulatory proceeding” of which you first receive notice during said Automatic Extended Reporting Period arising directly from a “wrongful act” occurring on or after the Retroactive Date, if any, shown in the Declarations and before the end of the “policy period” and which is otherwise insured by this Coverage Part; and

- b. Upon payment of the additional premium of 100% of the full annual premium associated with the relevant coverage, a Supplemental Extended Reporting Period of one year immediately following the expiration date of the Automatic Extended Reporting Period in which to give to us written notice of a “claim” or “regulatory proceeding” of which you first receive notice during said Supplemental Extended Reporting Period arising directly from a “wrongful act” occurring on or after the Retroactive Date, if any, shown in the Declarations and before the end of the “policy period” and which is otherwise insured by this Coverage Part.

To obtain the Supplemental Extended Reporting Period, you must request it in writing and pay the additional premium due, within 30 days after the “termination of coverage”. The additional premium for the Supplemental Extended Reporting Period will be fully earned at the inception of the Supplemental Extended Reporting Period. If we do not receive the written request as required, you may not exercise this right at a later date.

- c. The applicable Limits of Insurance for the Extended Reporting Periods will be part of, and not in addition to, the applicable Limits of Insurance for the immediately preceding “coverage term”.

## G. ADDITIONAL CONDITIONS

The following conditions apply in addition to the Common Policy Conditions:

### 1. Bankruptcy

The bankruptcy or insolvency of you or your estate, will not relieve you or us of any obligation under this Coverage Part.

### 2. Changes In Exposure

#### a. Acquisition Or Creation Of Another Organization

If before or during the “policy period”

- (1) You acquire securities or obtain right in an the organization or create another organization which, as a result of such acquisition or creation becomes a “subsidiary”; or
- (2) You acquire any organization through merger or consolidation;

then such organization will be covered under this Coverage Part but only with respect to “wrongful acts” or “loss” which occurred after the effective date of such acquisition or creation provided, with regard to paragraphs 2.a.(1) and 2.a.(2), you:

- (a) Give us written notice of the acquisition or creation of such organization within 90 days after the effective date of such action;
- (b) Obtain our written consent to extend the coverage provided by this Coverage Part to such organization; and
- (c) Upon obtaining our consent, pay us an additional premium.

#### b. Acquisition Of Named Insured

If during the “policy period”:

- (1) The “named insured” merges into or consolidates with another organization, such that the “named insured” is not the surviving organization; or
- (2) 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 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 Coverage Part will continue until the end of the “policy period”, but only with respect to “claims” arising out of “wrongful acts” or “loss” which occurred prior to the effective date of such merger, consolidation or acquisition.

The full annual premium for the “policy period” will be deemed to be fully earned immediately upon the occurrence of such merger, consolidation or acquisition of the “named insured”.

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. Cessation Of Subsidiaries**

If before or during the “policy period” an organization ceases to be a “subsidiary”, the coverage afforded under this Coverage Part 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” or “loss” which occurred prior to the date such organization ceased to be a “subsidiary”.

**3. Due Diligence**

You agree to use due diligence to prevent and mitigate “loss” insured under this Coverage Part. This includes, but is not limited to, complying with, and requiring your vendors to comply with, reasonable and industry-accepted protocols for:

- a. Providing and maintaining appropriate physical security for your premises, “computer systems” and hard copy files;
- b. Providing and maintaining appropriate computer and Internet security;
- c. Maintaining and updating at appropriate intervals backups of computer data;
- d. Protecting transactions, such as processing credit card, debit card and check payments; and
- e. Appropriate disposal of files containing “personally identifying information”, “personally sensitive information” or “third party corporate data”, including shredding hard copy files and destroying physical media used to store electronic data.

**4. Duties in the Event of a Claim, Regulatory Proceeding or Loss**

- a. If, during the “coverage term”, incidents or events occur which you reasonably believe may give rise to a “claim” or “regulatory proceeding” for which coverage may be provided hereunder, such belief being based upon either written notice from the potential claimant or the potential claimant’s representative, or notice of a complaint filed with a federal, state or local agency; or upon an oral “claim”, allegation or threat, you shall give written notice to us as soon as practicable and either:
  - (1) Anytime during the coverage term; or
  - (2) Anytime during the extended reporting periods (if applicable).
- b. If a “claim” or “regulatory proceeding” is brought against any “insured”, you must:
  - (1) Immediately record the specifics of the “claim” or “regulatory proceeding” and the date received;
  - (2) Provide us with written notice, as soon as practicable, but in no event more than 60 days after the date the “claim” or “regulatory proceeding” is first received by you;
  - (3) Immediately send us copies of any demands, notices, summonses or legal papers received in connection with the “claim” or “regulatory proceeding”;
  - (4) Authorize us to obtain records and other information;
  - (5) Cooperate with us in the investigation, settlement or defense of the “claim” or “regulatory proceeding”;
  - (6) Assist us, upon our request, in the enforcement of any right against any person or organization which may be liable to you because of “loss” or “defense costs” to which this insurance may also apply; and
  - (7) Not take any action, or fail to take any required action, that prejudices your rights or our rights with respect to such “claim” or “regulatory proceeding”.

If written notice is given to us during the “coverage term” or extended reporting periods (if applicable), pursuant to the above requirements, then any “claim” or “regulatory proceeding” which is subsequently made against any “insureds” and reported to us alleging, arising out of, based upon or attributable to such circumstances or alleging any related “wrongful act” to such circumstances, shall be considered made at the time such notice of such circumstances was first given.

- c. In the event of a “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion

threat” or “wrongful transfer event” insured under Coverage 1– Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion or Coverage 8 – Misdirected Payment Fraud, you and any involved “identity recovery insured” must see that the following are done:

- (1) Notify the police if a law may have been broken.
  - (2) Notify us as soon as possible, but in no event more than 60 days after the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat” or “wrongful transfer event”. Include a description of any property involved.
  - (3) As soon as possible, give us a description of how, when and where the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat” or “wrongful transfer event” occurred.
  - (4) As often as may be reasonably required, permit us to:
    - (a) Inspect the property proving the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat” or “wrongful transfer event”;
    - (b) Examine your books, records, electronic media and records and hardware;
    - (c) Take samples of damaged and undamaged property for inspection, testing and analysis; and
    - (d) Make copies from your books, records, electronic media and records and hardware.
  - (5) Send us signed, sworn proof of “loss” containing the information we request to investigate the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat” or “wrongful transfer event”. You must do this within 60 days after our request. We will supply you with the necessary forms.
  - (6) Cooperate with us in the investigation or settlement of the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat” or “wrongful transfer event”.
  - (7) If you intend to continue your business, you must resume all or part of your operations as quickly as possible.
  - (8) Make no statement that will assume any obligation or admit any liability for any “loss” for which we may be liable, without our prior written consent.
  - (9) Promptly send us any legal papers or notices received concerning the “loss”.
- d. We may examine any “insured” under oath, while not in the presence of any other “insured” and at such times as may be reasonably required, about any matter relating to this insurance or the “claim”, “regulatory proceeding” or “loss”, including an “insured’s” books and records. In the event of an examination, an “insured’s” answers must be signed.
- e. No “insured” may, except at their own cost, voluntarily make a payment, assume any obligation, or incur any expense without our prior written consent.

## 5. Identity Recovery Help Line

For assistance, if Coverage 2 – Identity Recovery applies, the “identity recovery insured” should call the **Identity Recovery Help Line** as shown in the Declarations.

The **Identity Recovery Help Line** can provide the “identity recovery insured” with:

- a. Information and advice for how to respond to a possible “identity theft”; and
- b. Instructions for how to submit a service request for Case Management Service and/or a claim form for Expense Reimbursement Coverage.

In some cases, we may provide Case Management services at our expense to an “identity recovery insured” prior to a determination that a covered “identity theft” has occurred. Our provision of such services is not an admission of liability under the Coverage Part. We reserve the right to deny further coverage or service if, after investigation, we determine that a covered “identity theft” has not occurred.

As respects Expense Reimbursement Coverage, the “identity recovery insured” must send to us, within 60 days after our request, receipts, bills or other records that support his or her claim for “identity recovery expenses”.

## 6. Legal Action Against Us

- a. No person or organization has the right to join us as a party or otherwise bring us into a suit asking for damages from a Named Insured.
- b. You may not bring any legal action against us involving a “claim” or “loss”:
  - (1) Unless you have complied with all the terms of this insurance;
  - (2) Until 90 days after you have filed proof of “claim” or “loss” with us; and
  - (3) Unless brought within two years from the date you discovered the “loss”.

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.

## 7. Legal Advice

We are not your legal advisor. Our determination of what is or is not insured under this Coverage Part does not represent advice or counsel from us about what you should or should not do.

## 8. Other Insurance

If there is other insurance that applies to the same “loss” this Coverage Part shall apply only as excess insurance after all other applicable insurance has been exhausted.

## 9. Pre-Notification Consultation

You agree to consult with us prior to the issuance of notification to “affected individuals”. We assume no responsibility under Coverage 1 – Data Compromise Response Expenses for any services promised to “affected individuals” without our prior agreement. If possible, this pre-notification consultation will also include the designated service provider(s) as agreed to under Additional Condition 12. Service Providers. You must provide the following at our pre-notification consultation with you:

- a. The exact list of “affected individuals” to be notified, including contact information.
- b. Information about the “personal data compromise” that may appropriately be communicated with “affected individuals”.
- c. The scope of services that you desire for the “affected individuals”. For example, coverage may be structured to provide for services in order to make those services available to more “affected individuals” without exceeding the available Data Compromise Response Expenses limit of insurance.

## 10. Representations

Any and all relevant provisions of this Coverage Part may be voidable by us in any case of fraud, intentional concealment, or misrepresentation of material fact by any “insured”.

## 11. Separation of Insureds

Except with respect to the limits of liability and any rights or duties specifically assigned to the first “named insured”, this insurance applies:

- a. As if each “named insured” were the only “named insured”; and
- b. Separately to each insured against whom a “claim” is made.

## 12. Service Providers

- a. We will only pay under this Coverage Part for services that are provided by service providers approved by us. You must obtain our prior approval for any service provider whose expenses you want covered under this Coverage Part. We will not unreasonably withhold such approval.
- b. Prior to the Pre-Notification Consultation described in the Pre-Notification Consultation Condition above, you must come to agreement with us regarding the service provider(s) to be used for the Notification to Affected Individuals and Services to Affected Individuals. We will suggest a service provider. If you prefer to use an alternate service provider, our coverage is subject to the following limitations:
  - (1) Such alternate service provider must be approved by us;

- (2) Such alternate service provider must provide services that are reasonably equivalent or superior in both kind and quality to the services that would have been provided by the service provider we had suggested; and
- (3) Our payment for services provided by any alternate service provider will not exceed the amount that we would have paid using the service provider we had suggested.

### 13. Services

The following conditions apply as respects any services provided to you or any “affected individual” or “identity recovery insured” by us, our designees or any service firm paid for in whole or in part under this Coverage Part:

- a. The effectiveness of such services depends on the cooperation and assistance of you, “affected individuals” and “identity recovery insureds”.
- b. All services may not be available or applicable to all individuals. For example, “affected individuals” and “identity recovery insureds” who are minors or foreign nationals may not have credit records that can be provided or monitored. Service in Canada will be different from service in the United States and Puerto Rico in accordance with local conditions.
- c. We do not warrant or guarantee that the services will end or eliminate all problems associated with the covered events.
- d. Except for the services of an “identity recovery case manager” under Coverage 2 – Identity Recovery, which we will provide directly, you will have a direct relationship with the professional service firms paid for in whole or in part under this Coverage Part. Those firms work for you.

### 14. Tie-In of Limits

As respects any “claim” or “regulatory proceeding” in which at least one person/entity claimed against is an “insured” under this Cyber Risk Coverage and at least one person/entity claimed against is an “insured” under another Cyber Risk Coverage issued to you by us (the Other Policy), the combined applicable limit of insurance provided under both this Cyber Risk Coverage and the Other Policy for all “losses” arising from such “claims” or “regulatory proceedings” combined shall not exceed the highest applicable limit of insurance under either this Cyber Risk Coverage or the Other Policy. This limitation shall apply even if both this Cyber Risk Coverage and the Other Policy have been triggered due to a “claim” or “regulatory proceeding” made against the same person/entity but alleging a “wrongful act” both in his, her or its capacity as an “insured” under the Other Policy and as an “insured” under this Cyber Risk Coverage.

### 15. Transfer of Control

- a. You may take over control of any outstanding “claim” or “regulatory proceeding” previously reported to us, but only if we, in our sole discretion, decide that you should, or if a court orders you to do so.
- b. Notwithstanding paragraph a., in all events, if the applicable limit of insurance is exhausted, we will notify you of all outstanding “claims” or “regulatory proceedings” and you will take over control of the defense. We will help transfer control of the “claims” and “regulatory proceedings” to you.
- c. We shall take whatever steps are necessary to continue the defense of any outstanding “claim” or “regulatory proceeding” and avoid a default judgment during the transfer of control to you. If we do so, we shall not waive or give up any of our rights. You shall pay all reasonable expenses we incur for taking such steps after the applicable limit of insurance is exhausted.

### 16. Transfer of Rights of Recovery Against Others to Us

If you or any person or organization to or for whom we make payment under this Coverage Part has rights to recover damages from another, those rights are transferred to us to the extent of our payment. You or that person or organization must do everything necessary to secure our rights and must do nothing after loss to impair them. However, you may waive your rights against another party in writing:

- a. Prior to a “loss”.
- b. After a “loss” only if, at time of the “loss”, that party is one of the following:
  - (1) Someone insured by this policy; or
  - (2) A business firm:
    - (a) Owned or controlled by you; or

- (b) That owns or controls you.

## H. DEFINITIONS

1. **“Affected Individual”** means any person whose “personally identifying information” or “personally sensitive information” is lost, stolen, accidentally released or accidentally published by a “personal data compromise” covered under this Coverage Part. This definition is subject to the following provisions:
  - a. “Affected individual” does not include any business or organization. Only an individual person may be an “affected individual”.
  - b. An “affected individual” may reside anywhere in the world.
2. **“Authorized Representative”** means a person or entity authorized by law or contract to act on behalf of an “identity recovery insured”.
3. **“Authorized Third Party User”** means a party who is not an “employee” or an “executive” of the “named insured” who is authorized by contract or other agreement to access the “computer system” for the receipt or delivery of services.
4. **“Bodily Injury”** means bodily injury, sickness or disease sustained by a person, including death resulting from any of these at any time.
5. **“Business Income and Extra Expense Loss”** means the loss of Business Income and Extra Expense actually incurred during the Period of Restoration.
  - a. As used in this definition, Business Income means the sum of:
    - (1) Net income (net profit or loss before income taxes) that would have been earned or incurred; and
    - (2) Continuing normal and necessary operating expenses incurred, including “employee” and “executive” payroll.
  - b. As used in this definition, Extra Expense means the additional cost you incur to operate your business over and above the cost that you normally would have incurred to operate your business during the same period had no computer attack occurred.
  - c. As used in this definition, Period of Restoration means the period of time that begins 8 hours after the time that the “computer attack” is discovered by you and continues until the earlier of:
    - (1) The date that all data restoration, data re-creation and system restoration directly related to the “computer attack” has been completed; or
    - (2) The date on which such data restoration, data re-creation and system restoration could have been completed with the exercise of due diligence and dispatch.
6. **“Claim”**
  - a. “Claim” means:
    - (1) A written demand for monetary damages or non-monetary relief, including injunctive relief;
    - (2) A civil proceeding commenced by the filing of a complaint;
    - (3) An arbitration proceeding in which such damages are claimed and to which the “insured” must submit or does submit with our consent;
    - (4) Any other alternative dispute resolution proceeding in which such damages are claimed and to which the “insured” must submit or does submit with our consent;
    - (5) A criminal proceeding commenced by:
      - (a) An arrest; or
      - (b) A return of an indictment, information or similar document; or
    - (6) A written request first received by you during the “coverage term” to toll or waive a statute of limitations relating to a potential “claim” described in a. (1) through (5) above, arising from a “wrongful act” or a series of “interrelated” “wrongful acts” allegedly committed by an “insured”, including any resulting appeal.
  - b. “Claim” does not mean or include:
    - (1) Any demand or action brought by or on behalf of someone who is:

- (a) Your “executive”;
  - (b) Your owner or part-owner; or
  - (c) A holder of your securities,
- in their capacity as such, whether directly, derivatively, or by class action. “Claim” will include proceedings brought by such individuals in their capacity as “affected individuals”, but only to the extent that the damages claimed are the same as would apply to any other “affected individual”; or
- (2) A “regulatory proceeding”.
- c. “Claim” includes a demand or proceeding arising from a “wrongful act” that is a “personal data compromise” only when the “personal data compromise” giving rise to the proceeding was covered under Coverage 1 – Data Compromise Response Expenses section of this Coverage Part, and you submitted a claim to us and provided notifications and services to “affected individuals” in consultation with us pursuant to Coverage 1 – Data Compromise Response Expenses in connection with such “personal data compromise”.
- 7. “Computer Attack”** means one of the following involving the “computer system”:
- a. An “unauthorized access incident”;
  - b. A “malware attack”; or
  - c. A “denial of service attack” against a “computer system”.
- 8. “Computer System”** means a computer or other electronic hardware that:
- a. Is owned or leased by you and operated under your control; or
  - b. Is operated by a third party service provider used for the purpose of providing hosted computer application services to you or for processing, maintaining, hosting or storing your electronic data, pursuant to a service contract with you for such services. However, such computer or other electronic hardware operated by such third party shall only be considered to be a “computer system” with respect to the specific services provided by such third party to you under such contract.
- 9. “Coverage Term”** means the following “individual increment, or in a multi-year policy period”, increments, of time, which comprise the “policy period” of this Coverage Part:
- a. The year commencing on the effective date of this Coverage Part shown in the Declarations, and if a multi-year “policy period”, each consecutive annual period thereafter, or portion thereof if any period is for a period of less than 12 months, constitute individual “coverage terms”. The last “coverage term” ends on the earlier of:
    - (1) The day the “policy period” shown in the Declarations ends; or
    - (2) The day the policy to which this Coverage Part is attached is terminated or cancelled.
  - b. However, if after the issuance of this Coverage Part, any “coverage term” is extended for an additional period of less than 12 months, that additional period of time will be deemed to be part of the last preceding “coverage term”.
- 10. “Coverage Territory”** means:
- a. With respect to Coverage 1 – Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion and Coverage 8 – Misdirected Payment Fraud, “coverage territory” means anywhere in the world.
  - b. With respect to Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability and Coverage 7 – Electronic Media Liability, “coverage territory” means anywhere in the world, however “claims” must be brought within the United States (including its territories and possessions) or Puerto Rico.
- 11. “Cyber Extortion Expenses”** means:
- a. The cost of a negotiator or investigator retained by you in connection with a “cyber extortion threat”; and
  - b. Any amount paid by you in response to a “cyber extortion threat” to the party that made the “cyber extortion threat” for the purposes of eliminating the “cyber extortion threat” when such expenses are



necessary and reasonable and arise directly from a “cyber extortion threat”. The payment of “cyber extortion expenses” must be approved in advance by us. We will not pay for “cyber extortion expenses” that have not been approved in advance by us. We will not unreasonably withhold our approval.

**12. “Cyber Extortion Threat” means:**

- a. “Cyber extortion threat” means a demand for money from you based on a credible threat, or series of related credible threats, to:
  - (1) Launch a “denial of service attack” against the “computer system” for the purpose of denying “authorized third party users” access to your services provided through the “computer system” via the Internet;
  - (2) Gain access to a “computer system” and use that access to steal, release or publish “personally identifying information”, “personally sensitive information” or “third party corporate data”;
  - (3) Alter, damage or destroy electronic data or software while such electronic data or software is stored within a “computer system”;
  - (4) Launch a “computer attack” against a “computer system” in order to alter, damage or destroy electronic data or software while such electronic data or software is stored within a “computer system”; or
  - (5) Cause you to transfer, pay or deliver any funds or property using a “computer system” without your authorization.
- b. “Cyber extortion threat” does not mean or include any threat made in connection with a legitimate commercial dispute.

**13. “Data Re-creation Costs”**

- a. “Data re-creation costs” means the costs of an outside professional firm hired by you to research, re-create and replace data that has been lost or corrupted and for which there is no electronic source available or where the electronic source does not have the same or similar functionality to the data that has been lost or corrupted.
- b. “Data re-creation costs” also include your actual business income and extra expense loss” arising from the lack of the lost or corrupted data during the time required to research, re-create and replace such data.
- c. “Data re-creation costs” does not mean or include costs to research, re-create or replace:
  - (1) Software programs or operating systems that are not commercially available; or
  - (2) Data that is obsolete, unnecessary or useless to you.

**14. “Data Restoration Costs”**

- a. “Data restoration costs” means the costs of an outside professional firm hired by you to replace electronic data that has been lost or corrupted. In order to be considered “data restoration costs”, such replacement must be from one or more electronic sources with the same or similar functionality to the data that has been lost or corrupted.
- b. “Data restoration costs” does not mean or include costs to research, re-create or replace:
  - (1) Software programs or operating systems that are not commercially available; or
  - (2) Data that is obsolete, unnecessary or useless to you.

**15. “Defense Costs”**

- a. “Defense costs” means reasonable and necessary expenses consented to by us resulting solely from the investigation, defense and appeal of any “claim” or “regulatory proceeding” against an “insured”. Such expenses may include premiums for any appeal bond, attachment bond or similar bond. However, we have no obligation to apply for or furnish such bond.
- b. “Defense costs” does not mean or include the salaries or wages of your “employees” or “executives”, or your loss of earnings.

**16. “Denial of Service Attack” means an intentional attack against a target computer or network of**

computers designed to overwhelm the capacity of the target computer or network in order to deny or impede authorized users from gaining access to the target computer or network through the Internet.

17. **“Electronic Media Incident”** means an allegation that the display of information in electronic form by you on a website resulted in:
- Infringement of another’s copyright, title, slogan, trademark, trade name, trade dress, service mark or service name;
  - Defamation against a person or organization that is unintended;
  - A violation of a person’s right of privacy, including false light and public disclosure of private facts;
  - Interference with a person’s right of publicity.
18. **“Employee”** means any natural person, other than an “executive”, who was, now is or will be:
- Employed on a full-time or part-time basis by you;
  - Furnished temporarily to you to substitute for a permanent “employee” on leave or to meet seasonal or short-term workload conditions;
  - 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 b.; or
  - Your volunteer worker, which includes unpaid interns.
19. **“Executive”** means any natural person who was, now is or will be:
- The owner of a sole proprietorship that is a “named insured”; or
  - A duly elected or appointed:
    - Director;
    - Officer;
    - Managing Partner;
    - General Partner;
    - Member (if a limited liability company);
    - Manager (if a limited liability company); or
    - Trustee,of a “named insured”.
20. **“Identity Recovery Case Manager”** means one or more individuals assigned by us to assist an “identity recovery insured” with communications we deem necessary for re-establishing the integrity of the personal identity of the “identity recovery insured”. This includes, with the permission and cooperation of the “identity recovery insured”, written and telephone communications with law enforcement authorities, governmental agencies, credit agencies and individual creditors and businesses.
21. **“Identity Recovery Expenses”** means the following when they are reasonable and necessary expenses that are incurred as a direct result of an “identity theft” suffered by an “identity recovery insured”:
- Re-Filing Costs**  
Costs for re-filing applications for loans, grants or other credit instruments that are rejected solely as a result of an “identity theft”.
  - Notarization, Telephone and Postage Costs**  
Costs for notarizing affidavits or other similar documents, long distance telephone calls and postage solely as a result of the “identity recovery insured’s” efforts to report an “identity theft” or amend or rectify records as to the “identity recovery insured’s” true name or identity as a result of an “identity theft”.
  - Credit Reports**  
Costs for credit reports from established credit bureaus.
  - Legal Costs**

Fees and expenses for an attorney approved by us for the following:

- (1) The defense of any civil suit brought against an "identity recovery insured".
- (2) The removal of any civil judgment wrongfully entered against an "identity recovery insured".
- (3) Legal assistance for an "identity recovery insured" at an audit or hearing by a governmental agency.
- (4) Legal assistance in challenging the accuracy of the "identity recovery insured's" consumer credit report.
- (5) The defense of any criminal charges brought against an "identity recovery insured" arising from the actions of a third party using the personal identity of the "identity recovery insured".

**e. Lost Wages**

Actual lost wages of the "identity recovery insured" for time reasonably and necessarily taken away from work and away from the work premises. Time away from work includes partial or whole work days. Actual lost wages may include payment for vacation days, discretionary days, floating holidays and paid personal days. Actual lost wages does not include sick days or any loss arising from time taken away from self-employment. Necessary time off does not include time off to do tasks that could reasonably have been done during non-working hours.

**f. Child and Elder Care Expenses**

Actual costs for supervision of children or elderly or infirm relatives or dependents of the "identity recovery insured" during time reasonably and necessarily taken away from such supervision. Such care must be provided by a professional care provider who is not a relative of the "identity recovery insured".

**g. Mental Health Counseling**

Actual costs for counseling from a licensed mental health professional. Such care must be provided by a professional care provider who is not a relative of the "identity recovery insured".

**h. Miscellaneous Unnamed Costs**

Any other reasonable costs necessarily incurred by a "identity recovery insured" as a direct result of the "identity theft".

- (1) Such costs include:
  - (a) Costs by the "identity recovery insured" to recover control over his or her personal identity.
  - (b) Deductibles or service fees from financial institutions.
- (2) Such costs do not include:
  - (a) Costs to avoid, prevent or detect "identity theft" or other loss.
  - (b) Money lost or stolen.
  - (c) Costs that are restricted or excluded elsewhere in this Coverage Part or policy.

**22. "Identity Recovery Insured" means the following:**

- a. When the entity insured under this Coverage Part is a sole proprietorship, the "identity recovery insured" is the individual person who is the sole proprietor of the "named insured".
- b. When the "named insured" under this Coverage Part is a partnership, the "identity recovery insureds" are the current partners.
- c. When the "named insured" under this Coverage Part is a corporation or other form of organization, other than those described in a. or b. above, the "identity recovery insureds" are all individuals having an ownership position of 20% or more of the insured entity. However, if, and only if, there is no one who has such an ownership position, then the "identity recovery insured" will be:
  - (1) The chief executive of the insured entity; or
  - (2) As respects a religious institution, the senior ministerial employee.
- d. The legally recognized spouse of any individual described in a., b. or c. above.

An "identity recovery insured" must always be an individual person. If the "named insured" under this

Coverage Part is a legal entity, that legal entity is not an “identity recovery insured”.

**23. “Identity Theft”**

- a. “Identity theft” means the fraudulent use of “personally identifying information”. This includes fraudulently using such information to establish credit accounts, secure loans, enter into contracts or commit crimes.
- b. “Identity theft” does not mean or include the fraudulent use of a business name, d/b/a or any other method of identifying a business activity.

**24. “Insured”**

- a. With respect to Coverage 1 – Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion and Coverage 8 – Misdirected Payment Fraud, “insured” means any “named insured”.
- b. With respect to Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability and Coverage 7 – Electronic Media Liability, “insured” means:
  - (1) Any “named insured”; and
  - (2) Any “employee” or “executive” of a “named insured”, but:
    - (a) Only for the conduct of the “named insured’s” business within the scope of his or her employment or duties as an “employee” or “executive”; and
    - (b) Such “employee” or “executive” will not be an “insured” to the extent his or her actions or omissions are criminal, fraudulent, dishonest or constitute an intentional or knowing violation of the law.

**25. “Interrelated”** means all events or incidents that have as a common nexus any:

- a. Fact, circumstance, situation, event, transaction, cause; or
- b. Series of causally connected facts, circumstances, situations, events, transactions or causes.

**26. “Loss”**

- a. With respect to Coverage 1 – Data Compromise Response Expenses “loss” means those expenses enumerated in Coverage 1 – Data Compromise Response Expenses paragraph b.
- b. With respect to Coverage 2 – Identity Recovery, “loss” means those expenses enumerated in Coverage 2 – Identity Recovery, paragraph b.
- c. With respect to Coverage 3 – Computer Attack, “loss” means those expenses enumerated in Coverage 3 – Computer Attack, paragraph b.
- d. With respect to Coverage 4 – Cyber Extortion, “loss” means “cyber extortion expenses”.
- e. With respect to Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability and Coverage 7 – Electronic Media Liability, “loss” means “defense costs” and “settlement costs”.
- f. With respect to Coverage 8 – Misdirected Payment Fraud, “loss” means “wrongful transfer costs”.

**27. “Malware Attack”**

- a. “Malware attack” means an attack that damages a “computer system” or data contained therein arising from malicious code, including viruses, worms, Trojans, spyware and keyloggers.
- b. “Malware attack” does not mean or include damage from shortcomings or mistakes in legitimate electronic code or damage from code installed on your “computer system” during the manufacturing process or normal maintenance.

**28. “Named Insured”** means the entity or entities shown in the Declarations as a Named Insured and their “subsidiaries”.

**29. “Network Security Incident”** means a negligent security failure or weakness with respect to a “computer system” which allowed one or more of the following to happen:

- a. The unintended propagation or forwarding of malware, including viruses, worms, Trojans, spyware and keyloggers. Malware does not include shortcomings or mistakes in legitimate electronic code.
- b. The unintended abetting of a “denial of service attack” against one or more other systems.
- c. The unintended loss, release or disclosure of “third party corporate data”.

- d. The inability of an “authorized third party user” to access a “computer system” due to a “malware attack”, a “denial of service attack” against a “computer system” or an “unauthorized access incident”.
- 30. “Personal Data Compromise”** means the loss, theft, accidental release or accidental publication of “personally identifying information” or “personally sensitive information” as respects one or more “affected individuals”. If the loss, theft, accidental release or accidental publication involves “personally identifying information”, such loss, theft, accidental release or accidental publication must result in or have the reasonable possibility of resulting in the fraudulent use of such information. This definition is subject to the following provisions:
- a. At the time of the loss, theft, accidental release or accidental publication, the “personally identifying information” or “personally sensitive information” need not be at the insured premises but must be in the direct care, custody or control of:
    - (1) You; or
    - (2) A professional entity with which you have a direct relationship and to which you (or an “affected individual” at your direction) have turned over (directly or via a professional transmission or transportation provider) such information for storage, processing, transmission or transportation of such information.
  - b. “Personal data compromise” includes disposal or abandonment of “personally identifying information” or “personally sensitive information” without appropriate safeguards such as shredding or destruction, provided that the failure to use appropriate safeguards was accidental and not reckless or deliberate.
  - c. “Personal data compromise” includes situations where there is a reasonable cause to suspect that such “personally identifying information” or “personally sensitive information” has been lost, stolen, accidentally released or accidentally published, even if there is no firm proof.
  - d. All incidents of “personal data compromise” that are discovered at the same time or arise from the same cause will be considered one “personal data compromise”.
- 31. “Personally Identifying Information”**
- a. “Personally identifying information” means information including, but not limited to, information that could be used to commit fraud or other illegal activity involving credit, access to health care or identity of an “affected individual” or “identity recovery insured”. This includes, but is not limited to, Social Security numbers or account numbers.
  - b. “Personally identifying information” does not mean or include information that is otherwise available to the public, such as names and addresses.
- 32. “Personally Sensitive Information”**
- a. “Personally sensitive information” means private information specific to an individual the release of which requires notification of “affected individuals” under any applicable law.
  - b. “Personally sensitive information” does not mean or include “personally identifying information”.
- 33. “Policy Period”** means the period commencing on the effective date shown in the Coverage Part Declarations. The “policy period” ends on the expiration date or the cancellation date of this Coverage Part, whichever comes first.
- 34. “Pollutants”** include, but are not limited to, any solid, liquid, gaseous, biological, radiological or thermal irritant or contaminant, including smoke, vapor, dust, fibers, mold, spores, fungi, germs, soot, fumes, asbestos, acids, alkalis, chemicals, and waste. Waste includes, but is not limited to, materials to be recycled, reconditioned or reclaimed and nuclear materials.
- 35. “Property Damage”** means
- a. Physical injury to or destruction of tangible property including all resulting loss of use; or
  - b. Loss of use of tangible property that is not physically injured.
- 36. “Regulatory Proceeding”** means an investigation, demand or proceeding alleging a violation of law or regulation brought by, or on behalf of, the Federal Trade Commission, Federal Communications Commission or other administrative or regulatory agency, or any federal, state, local or foreign governmental entity in such entity’s regulatory or official capacity.

### 37. "Settlement Costs"

- a. "Settlement costs" means the following, when they arise from a "claim":
  - (1) Damages (including punitive and exemplary damages and the multiple portion of any multiplied damage award), judgments or settlements; and
  - (2) Attorney's fees and other litigation costs added to that part of any judgment paid by us, when such fees and costs are awarded by law or court order; and
  - (3) Pre-judgment interest on that part of any judgment paid by us.
- b. "Settlement costs" does not mean or include:
  - (1) Civil or criminal fines or penalties imposed by law, except for civil fines and penalties expressly covered under Coverage 1 – Data Compromise Response Expenses;
  - (2) Taxes; or
  - (3) Matters which may be deemed uninsurable under the applicable law.
- c. With respect to fines and penalties and punitive, exemplary and multiplied damages, the law of the jurisdiction most favorable to the insurability of those fines, penalties or damages will control for the purpose of resolving any dispute between us and any "insured" regarding whether the fines, penalties or damages specified in this definition above are insurable under this Coverage Part, provided that such jurisdiction:
  - (1) Is where those fines, penalties or damages were awarded or imposed;
  - (2) Is where any "wrongful act" took place for which such fines, penalties or damages were awarded or imposed;
  - (3) Is where you are incorporated or you have your principal place of business; or
  - (4) Is where we are incorporated or have our principal place of business.

38. "Subsidiary" means an organization in which more than fifty (50) percent (%) 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 owned, in any combination, by one or more named insured(s).

### 39. "System Restoration Costs"

- a. "System restoration costs" means the costs of an outside professional firm hired by you to do any of the following in order to restore your computer system to the level of functionality it had immediately prior to the "computer attack":
  - (1) Replace or reinstall computer software programs;
  - (2) Remove any malicious code; and
  - (3) Configure or correct the configuration of your computer system.
- b. "System restoration costs" does not mean or include:
  - (1) Costs to increase the speed, capacity or utility of a "computer system" beyond what existed immediately prior to the "computer attack"; or
  - (2) Labor costs of your "employees" or "executives".

### 40. "Termination of Coverage" means:

- a. You or we cancel this coverage;
- b. You or we refuse to renew this coverage; or
- c. We renew this coverage on an other than claims-made basis or with a retroactive date later than the Retroactive Date, if any, shown in the Declarations.

### 41. "Third Party Corporate Data"

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

- b. "Third party corporate data" does not mean or include "personally identifying information" or "personally sensitive information".

**42. "Unauthorized Access Incident"** means the gaining of access to a "computer system" by:

- a. An unauthorized person or persons; or
- b. An authorized person or persons for unauthorized purposes.

**43. "Wrongful Act"**

- a. With respect to Coverage 5 – Data Compromise Liability, "wrongful act" means a "personal data compromise".
- b. With respect to Coverage 6 – Network Security Liability, "wrongful act" means a "network security incident".
- c. With respect to Coverage 7 – Electronic Media Liability, "wrongful act" means an "electronic media incident".

**44. "Wrongful transfer costs"** means the amount fraudulently obtained from the "insured". "Wrongful transfer costs" include the direct financial loss only. "Wrongful transfer costs" do not include any of the following:

- a. Other expenses that arise from the "wrongful transfer event";
- b. Indirect loss, such as "bodily injury", lost time, lost wages, identity recovery expenses or damaged reputation;
- c. Any interest, time value or potential investment gain on the amount of financial loss; or
- d. Any portion of such amount that has been or can reasonably be expected to be reimbursed by a third party, such as a financial institution.

**45. "Wrongful transfer event"**

- a. "Wrongful transfer event" means an intentional and criminal deception of an "insured" or a financial institution with which the "insured" has an account. The deception must be perpetrated by a person who is not an employee, using email, facsimile or telephone communications to induce the "insured" or the financial institution to send money or divert a payment. The deception must result in direct financial loss to an "insured".
- b. "Wrongful transfer event" does not mean or include any occurrence:
  - (1) In which the "insured" is threatened or coerced to send money or divert a payment; or
  - (2) Arising from a dispute or a disagreement over the completeness, authenticity or value of a product, a service or a financial instrument.

Named Insured: Sample Policy				
Policy Number: 01-CY-0005511657-00	Transaction Effective Date: 10/01/2021	Policy Period: 10/01/2021 to 10/01/2022	Issue Date: 09/17/2021	Ref. No.: N/A

## Additional Insured – Pursuant To A Contract

This endorsement changes the policy. Please read it carefully.

This endorsement modifies insurance provided under the following:

### Cyber Risk Coverage Form

A. The following is added to Section H. **DEFINITIONS**:

“Additional insured” means any person or entity that the “named insured” has agreed by a written contract to add as an “additional insured” under this policy for a “personal data compromise” under Coverage 5 – Data Compromise Liability, a “network security incident” under Coverage 6 – Network Security Liability or an “electronic media incident” under Coverage 7 – Electronic Media Liability that took place after the “named insured” and “additional insured” entered into the written contract and for any “personal data compromise”, “network security incident”, or “electronic media incident” committed by, on behalf of, or at the direction of the “named insured” subject to the lesser of the limits of insurance required by the contract or the applicable limits of insurance of this policy.

B. Section H. **DEFINITIONS**, item 24. “Insured” paragraph (1) is deleted and replaced with the following:

- b. With respect to Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability and Coverage 7 – Electronic Media Liability, “insured” means:
- (1) Any “named insured”;
  - (2) Any “employee” or “executive” of a “named insured”, but:
    - (a) Only for the conduct of the “named insured’s” business within the scope of his or her employment or duties as an “employee” or “executive”; and
    - (b) Such “employee” or “executive” will not be an “insured” to the extent his or her actions or omissions are criminal, fraudulent, dishonest or constitute an intentional or knowing violation of the law; and
  - (3) An “additional insured”.

C. The following is added to section **G. ADDITIONAL CONDITIONS**, item 8. Other Insurance:

Notwithstanding the above, if the “named insured” has contracted to provide primary insurance to an “additional insured” then this policy shall be considered primary insurance to any other insurance provided by or for the benefit of the “additional insured”.

ALL OTHER PROVISIONS OF THIS POLICY APPLY.



Named Insured: Sample Policy				
Policy Number: 01-CY-0005511657-00	Transaction Effective Date: 10/01/2021	Policy Period: 10/01/2021 to 10/01/2022	Issue Date: 09/17/2021	Ref. No.: N/A

## Business Identity Theft Liability

This endorsement changes the policy. Please read it carefully.

This endorsement modifies insurance provided under the following:

### Cyber Risk Coverage Form

A. The following is added to Section **A. COVERAGE**:

#### Business Identity Theft Liability

- a. Business Identity Theft Liability coverage applies only if all of the following conditions are met:
  - (1) During the “coverage term” or any applicable Extended Reporting Period, you first receive notice of a “claim” or “regulatory proceeding” which arises from a “fraud-induced default” or “a fraudulent filing”.  
The “fraud induced default” or “fraudulent filing” and the underlying “business identity theft” must:
    - (a) Take place on or after the Retroactive Date, if any, shown in the Declarations and before the end of the “policy period”; and
    - (b) Take place in the “coverage territory”; and
  - (2) Such “claim” or “regulatory proceeding” is reported to us as soon as practicable, but in no event more than 60 days after the date it is first received by you.
- b. If the conditions listed in a. above have been met, then we will pay on behalf of the “insured”:
  - (1) “Loss” directly arising from the “claim”; or
  - (2) “Defense costs” directly arising from a “regulatory proceeding”.
- c. All “claims” and “regulatory proceedings” arising from a single “business identity theft” or “interrelated” “business identity thefts” will be deemed to have been made at the time that notice of the first of those “claims” or “regulatory proceedings” is received by you.

B. Section **D. DEDUCTIBLES**, item 2., paragraph b. is deleted and replaced with the following:

- b. “Loss” resulting from the same “wrongful act” or “interrelated” “wrongful acts” insured under Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability, Coverage 7 – Electronic Media Liability, or Business Identity Theft Liability coverage.

C. The following is added to Section **E. DEFENSE AND SETTLEMENT**:

The following provisions are applicable to the Business Identity Theft Liability coverage.

D. The following is added to Section **F. EXTENDED REPORTING PERIODS**:

The following provisions are applicable to the Business Identity Theft Liability coverage.

E. Section **H. DEFINITIONS**, item **10. “Coverage Territory”**, paragraph b. is deleted and replaced with the following:

- b. With respect to Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability, Coverage 7 – Electronic Media Liability, and Business Identity Theft Liability, “coverage territory” means anywhere in the world, however “claims” must be brought within the United States (including its territories and possessions) or Puerto Rico.

F. Section **H. DEFINITIONS**, item **24. “Insured”**, paragraph b. is deleted and replaced with the following:

- b. With respect to Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability, Coverage 7 – Electronic Media Liability, and Business Identity Theft Liability coverage, “insured” means:
- (1) Any “named insured”; and
  - (2) Any “employee” or “executive” of a “named insured”, but:
    - (a) Only for the conduct of the “named insured’s” business within the scope of his or her employment or duties as an “employee” or “executive”; and
    - (b) Such “employee” or “executive” will not be an “insured” to the extent his or her actions or omissions are criminal, fraudulent, dishonest or constitute an intentional or knowing violation of the law.

G. Section **H. DEFINITIONS**, item **26. “Loss”**, paragraph e. is deleted and replaced with the following:

- e. With respect to Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability, Coverage 7 – Electronic Media Liability, and Business Identity Theft Liability coverage, “loss” means “defense costs” and “settlement costs”.

H. Section **H. DEFINITIONS**, item **36. “Regulatory Proceeding”** is deleted and replaced with the following:

- 36. “Regulatory Proceeding”** means an investigation, demand or proceeding alleging a violation of law or regulation brought by, or on behalf of, the Internal Revenue Service, Federal Trade Commission, Federal Communication Commission or other administrative or regulatory agency or any federal, state, local or foreign governmental entity in such entity’s regulatory or official capacity.

I. Section **H. DEFINITIONS**, item **37. “Settlement Costs”** is deleted and replaced with the following:

**37. “Settlement Costs”**

- a. “Settlement costs” means the following, when they arise from a “claim” or “regulatory proceeding”:
- (1) Damages (including punitive and exemplary damages and the multiple portion of any multiplied damage award), judgments or settlements; and
  - (2) Attorney’s fees and other litigation costs added to that part of any judgment paid by us, when such fees and costs are awarded by law or court order; and
  - (3) Pre-judgment interest on that part of any judgment paid by us.
- b. “Settlement costs” does not mean or include:
- (1) Civil or criminal fines or penalties imposed by law, except for civil fines and penalties expressly covered under Coverage 1 – Data Compromise Response Expenses;
  - (2) Taxes; or
  - (3) Matters which may be deemed uninsurable under the applicable law.
- c. With respect to fines and penalties and punitive, exemplary and multiplied damages, the law of the jurisdiction most favorable to the insurability of those fines, penalties or damages will control for the purpose of resolving any dispute between us and any “insured” regarding whether the fines, penalties or damages specified in this definition above are insurable under this Coverage Part, provided that such jurisdiction:
- (1) Is where those fines, penalties or damages were awarded or imposed;

- (2) Is where any “wrongful act” took place for which such fines, penalties or damages were awarded or imposed;
- (3) Is where you are incorporated or you have your principal place of business; or
- (4) Is where we are incorporated or have our principal place of business.

J. The following is added to Section **H. DEFINITIONS**, item **43. “Wrongful Act”**:

With respect to Business Identity Theft Liability coverage, “wrongful act” means a “fraud-induced default” or “fraudulent filing”.

K. The following are added to Section **H. DEFINITIONS**:

**“Business Identity Theft”**

- a. “Business identity theft” means the fraudulent use of the employer identification number or other method of identifying the “named insured” without the “named insured’s” knowledge, cooperation or consent.
- b. “Business identity theft” includes fraudulently impersonating the “named insured” in order to establish credit accounts, secure loans, order goods, file tax returns or enter into contracts.
- c. “Business identity theft” does not include:
  - (1) Fraudulent activity by any “executive”, “employee” or “independent contractor” of the “named insured”.
  - (2) “Business identity theft” does not include the fraudulent use of a social security number or any other method of identifying an individual person.

**“Fraud-Induced Default”** means a default by you on a financial obligation when such financial obligation was created as part of a business identity theft.

**“Fraudulent Filing”** means the filing of a fraudulent tax return when such tax return was created as part of a “business identity theft”.

ALL OTHER PROVISIONS OF THIS POLICY APPLY.

Named Insured: Sample Policy				
Policy Number: 01-CY-0005511657-00	Transaction Effective Date: 10/01/2021	Policy Period: 10/01/2021 to 10/01/2022	Issue Date: 09/17/2021	Ref. No.: N/A

## Costs of Forensic Accountant

This endorsement changes the policy. Please read it carefully.

This endorsement modifies insurance provided under the following:

### Cyber Risk Coverage Form

The following is added to Section **H. DEFINITIONS**, item **5. "Business Income and Extra Expense Loss"**:

"Business income and extra expense loss" also includes your reasonable and necessary costs to retain a third party forensic accounting firm required to determine the loss of Business Income and Extra Expense actually incurred by you during the Period of Restoration.

ALL OTHER PROVISIONS OF THIS POLICY APPLY.

Sample

Named Insured: Sample Policy				
Policy Number: 01-CY-0005511657-00	Transaction Effective Date: 10/01/2021	Policy Period: 10/01/2021 to 10/01/2022	Issue Date: 09/17/2021	Ref. No.: N/A

## Cryptojacking

This endorsement changes the policy. Please read it carefully.

This endorsement modifies insurance provided under the following:

### Cyber Risk Coverage Form

A. The following is added to Section **A. COVERAGE**:

#### Cryptojacking

a. Cryptojacking applies only if all of the following conditions are met:

- (1) There has been a “cryptojacking event”; and
- (2) Such “cryptojacking event” took place in the “coverage territory”; and
- (3) Such “cryptojacking event” is first discovered by you during the “coverage term”; and
- (4) Such “cryptojacking event” is reported to us within 60 days after the date it is first discovered by you.

b. If all of the conditions stated in a. above have been met, then we will pay your necessary and reasonable “loss” directly arising from such “cryptojacking event”.

B. Section **C. LIMITS OF INSURANCE**, item **4. Application of Limits**, paragraph a. is deleted and replaced with the following:

a. A “computer attack”, “cyber extortion threat”, “personal data compromise”, “identity theft”, “wrongful transfer event” or “cryptojacking event” may be first discovered by you in one “coverage term” but it may cause insured “loss” in one or more subsequent “coverage terms”. If so, all insured “loss” arising from such “computer attack”, “cyber extortion threat”, “personal data compromise”, “identity theft”, “wrongful transfer event” or “cryptojacking event” will be subject to the limit of insurance applicable to the “coverage term” when the “computer attack”, “cyber extortion threat”, “personal data compromise”, “identity theft”, “wrongful transfer event” or “cryptojacking event” was first discovered by you.

C. Section **D. DEDUCTIBLES**, item 2., paragraph a. is deleted and replaced with the following:

a. “Loss” arising from the same insured event or “interrelated” insured events under Coverage 1 – Data Compromise Response Expenses, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud or Cryptojacking coverage.

D. Section **G. ADDITIONAL CONDITIONS**, item **4. Duties in the Event of a Claim, Regulatory Proceeding or Loss**, paragraph c. is deleted and replaced with the following:

c. In the event of a “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “cryptojacking event” insured under Coverage 1– Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud or Cryptojacking coverage, you and any involved “identity recovery insured” must see that the following are done:

- (1) Notify the police if a law may have been broken.
- (2) Notify us as soon as possible, but in no event more than 60 days after the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “cryptojacking event”. Include a description of any property involved.
- (3) As soon as possible, give us a description of how, when and where the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “cryptojacking event” occurred.
- (4) As often as may be reasonably required, permit us to:
  - (a) Inspect the property proving the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “cryptojacking event”;
  - (b) Examine your books, records, electronic media and records and hardware;
  - (c) Take samples of damaged and undamaged property for inspection, testing and analysis; and
  - (d) Make copies from your books, records, electronic media and records and hardware.
- (5) Send us signed, sworn proof of “loss” containing the information we request to investigate the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “cryptojacking event”. You must do this within 60 days after our request. We will supply you with the necessary forms.
- (6) Cooperate with us in the investigation or settlement of the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “cryptojacking event”.
- (7) If you intend to continue your business, you must resume all or part of your operations as quickly as possible.
- (8) Make no statement that will assume any obligation or admit any liability, for any “loss” for which we may be liable, without our prior written consent.
- (9) Promptly send us any legal papers or notices received concerning the “loss”.

E. Section **H. DEFINITIONS**, item 11 “**Coverage Territory**” paragraph a. is deleted and replaced with the following:

- a. With respect to Coverage 1 – Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud, and Cryptojacking coverage, “coverage territory” means anywhere in the world.

F. Section **H. DEFINITIONS**, item 24. “**Insured**”, paragraph a. is deleted and replaced with the following:

- a. With respect to Coverage 1 – Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud, and Cryptojacking coverage, “insured” means any “named insured”.

G. The following is added to Section **H. DEFINITIONS**, item 26. “**Loss**”:

With respect to Cryptojacking coverage, “loss” means “utility bill overage expenses”.

H. The following are added to Section **H. DEFINITIONS**:

“**Cryptojacking Event**” means an “unauthorized access incident” or “malware attack” carried out for the purposes of mining cryptocurrency that causes you to incur “utility bill overage expenses”.

“**Utility Bill Overage Expenses**”

- a. “Utility bill overage expenses” means additional expenses you incur to operate your business over and above the cost that you normally would have incurred to operate your business during the same period had no “cryptojacking event” occurred, provided that such additional expenses are:

- (1) Incurred under a contract between you and the Utility Provider. Such contract must be in writing and have a date of execution prior to the “cryptojacking event”.
  - (2) Billed to you by the Utility Provider via written invoices that include details of utility usage or consumption.
- b. “Utility bill overage expenses” does not mean or include any expenses that are:
- (1) Not incurred during the “policy period”; or
  - (2) Charged at a flat or fixed fee that does not fluctuate with usage.
- c. As used in this definition, Utility Provider means an electrical, internet, natural gas or oil service provider.

**ALL OTHER PROVISIONS OF THIS POLICY APPLY.**

Sample

Named Insured: Sample Policy				
Policy Number: 01-CY-0005511657-00	Transaction Effective Date: 10/01/2021	Policy Period: 10/01/2021 to 10/01/2022	Issue Date: 09/17/2021	Ref. No.: N/A

## Extended Income Recovery

This endorsement changes the policy. Please read it carefully.

This endorsement modifies insurance provided under the following:  
**Cyber Risk Coverage Form**

A. The following is added to Section **A. COVERAGE**, item **3. Computer Attack**, paragraph b.:

### Extended Income Recovery

We will pay your actual "extended income loss" if you suffer a covered "business income and extra expense loss" resulting from a "computer attack" on a "computer system" owned or leased by you and operated under your control.

B. Section **C. LIMITS OF INSURANCE**, item **3. Coverage Sublimits**, paragraph c. **Coverage 3 Sublimits** is deleted and replaced with the following:

### c. Coverage 3 Sublimits

The most we will pay under Coverage 3 – Computer Attack for Data Re-Creation, Loss of Business and Crisis Management, Coverage 3 Sublimits arising from any one "computer attack" is the applicable sublimit for each of those coverages shown in the Declarations. The most we will pay under Coverage 3 – Computer Attack for Contingent Loss of Business coverage and Extended Income Recovery coverage for "loss" arising from any one "computer attack" is the Loss of Business sublimit shown in the Declarations. These sublimits are part of, and not in addition to, the aggregate limit for Coverage 3 – Computer Attack shown in the Declarations.

C. The following are added to section **H. DEFINITIONS**:

**"Extended Income Loss"** means your actual "business income and extra expense loss" incurred during the "extended recovery period".

### **"Extended Recovery Period"**

- a. "Extended Recovery Period" means the period shown in the Declarations for Extended Recovery Period immediately following the end of the Period of Restoration.
- b. As used in this definition, Period of Restoration means the period of time that begins after the "waiting period" and continues until the earlier of:
  - (1) The date that all data restoration, data re-creation and system restoration directly related to the "computer attack" has been completed;
  - (2) The date on which such data restoration, data re-creation and system restoration could have been completed with the exercise of due diligence and dispatch; or
  - (3) The "maximum period of restoration" has elapsed.

ALL OTHER PROVISIONS OF THIS POLICY APPLY.



Named Insured: Sample Policy				
Policy Number: 01-CY-0005511657-00	Transaction Effective Date: 10/01/2021	Policy Period: 10/01/2021 to 10/01/2022	Issue Date: 09/17/2021	Ref. No.: N/A

## Full Media Liability

This endorsement changes the policy. Please read it carefully.

This endorsement modifies insurance provided under the following:

### Cyber Risk Coverage Form

A. Section **A. COVERAGE**, item **7. Electronic Media Liability**, is deleted and replaced with the following:

#### 7. Media Liability

- a. Coverage 7 – Media Liability applies only if all of the following conditions are met:
  - (1) During the “coverage term” or any applicable Extended Reporting Period, you first receive notice of a “claim” which arises from a “media incident” that:
    - (a) Took place on or after the Retroactive Date, if any, shown in the Declarations and before the end of the “policy period”; and
    - (b) Took place in the “coverage territory”; and
  - (2) Such “claim” is reported to you as soon as practicable, but in no event more than 60 days after the date it is first received by you.
- b. If the conditions listed in (a) above have been met, we will pay on behalf of the “insured” “loss” directly arising from the “claim”.
- c. All “claims” arising from a single “media incident” or “unrelated” “media incidents” will be deemed to have been made at the time that notice of the first of those “claims” is received by you.

B. Section **H. DEFINITIONS**, item **17. “Electronic Media Incident”** is deleted and replaced with the following:

#### 17. “Media Incident” means an allegation that the display of information by you resulted in:

- a. Infringement of another’s copyright, title, slogan, trademark, trade name, trade dress, service mark or service name;
- b. Defamation against a person or organization that is unintended;
- c. A violation of a person’s right of privacy, including false light and public disclosure of private facts;
- d. Interference with a person’s right of publicity.

C. Section **H. DEFINITIONS**, item **43. “Wrongful Act”**, paragraph c. is deleted and replaced with the following:

- c. With respect to Coverage 7 – Media Liability, “wrongful act” means a “media incident”

D. For the purposes of this endorsement only, wherever the term Electronic Media Liability is used in the Cyber Risk Coverage Form it shall be replaced with the term Media Liability.

ALL OTHER PROVISIONS OF THIS POLICY APPLY.

Named Insured: Sample Policy				
Policy Number: 01-CY-0005511657-00	Transaction Effective Date: 10/01/2021	Policy Period: 10/01/2021 to 10/01/2022	Issue Date: 09/17/2021	Ref. No.: N/A

## HSB Total Cyber™ Enhancement Endorsement

This endorsement changes the policy. Please read it carefully.

This endorsement modifies insurance provided under the following:

### Cyber Risk Coverage Form

- A. Section **A. COVERAGE**, item **1. Data Compromise Response Expenses**, paragraph b.(1) **Forensic IT Review** is deleted and replaced with the following:

#### (1) Forensic IT Review

Professional information technologies review if needed to determine, within the constraints of what is possible and reasonable, the nature and extent of the “personal data compromise” and the number and identities of the “affected individuals”. This includes, when necessary, the cost of a qualified Payment Card Industry Forensic Investigator.

This does not include costs to analyze, research or determine any of the following:

- (a) Vulnerability assessments, penetration testing or physical security; or
- (b) The nature or extent of loss or damage to data that is not “personally identifying information” or “personally sensitive information”.

If there is reasonable cause to suspect that a covered “personal data compromise” may have occurred, we will pay for costs covered under Forensic IT Review, even if it is eventually determined that there was no covered “personal data compromise”. However, once it is determined that there was no covered “personal data compromise”, we will not pay for any further costs.

- B. Section **A. COVERAGE**, item **1. Data Compromise Response Expenses**, paragraph b. (6) **Regulatory Fines and Penalties** is deleted and replaced with the following:

#### (6) Regulatory Fines and Penalties

Any fine or penalty imposed by law, to the extent such fine or penalty is legally insurable under the law of the applicable jurisdiction. This includes, but is not limited to, fines and penalties imposed for the violation of the European Union General Data Protection Regulation, the California Consumer Privacy Act and similar laws.

- C. Section **A. COVERAGE**, item **3. Computer Attack**, paragraph b.(4) **Loss of Business** is deleted and replaced with the following:

#### (4) Loss of Business

We will pay your actual “business income and extra expense loss” resulting from a “computer attack” on your “computer system”. This includes your actual “business income and extra expense loss” caused by a voluntary shutdown of your “computer system” in connection with your reasonable efforts to stop, mitigate the effects of or recover from such a “computer attack”.

- D. The following is added to Section **A. COVERAGE**, item **8. Misdirected Payment Fraud**:

#### Computer Fraud

- a. This Computer Fraud coverage applies only if all of the following conditions are met:
  - (1) There has been a “computer fraud event” against you; and
  - (2) Such “computer fraud event” took place in the “coverage territory”; and
  - (3) Such “computer fraud event” is first discovered by you during the “coverage term”; and
  - (4) Such “computer fraud event” is reported to us within 60 days after the date it is first discovered by you; and
  - (5) Such “computer fraud event” is reported in writing by you to the police.
- b. If the conditions listed in a. above have been met, then we will pay your necessary and reasonable “computer fraud costs” arising directly from the “computer fraud event”.

E. The following is added to Section **A. COVERAGE**:

**Reward Payment Reimbursement**

- a. This Reward Payment Reimbursement coverage applies only if all of the following conditions are met:
  - (1) There has been a “reward payment qualifying event” in response to which you have offered and made “reward payments”; and
  - (2) We agree to such “reward payments” in writing prior to the “reward payments” being offered or paid; and
  - (3) Such “reward payments” lead to the arrest and conviction of any perpetrator(s) of a “reward payment qualifying event”; and
  - (4) Such “reward payments” are offered and paid prior to the earlier of:
    - (a) six months after the “reward payment qualifying event” or
    - (b) expiration of the policy term
- b. If the conditions listed in a. above have been met, then we will reimburse you for any necessary and reasonable “reward payment” arising directly from such “reward payment qualifying event”.

F. Section **B. EXCLUSIONS**, item **1. General Exclusions**, paragraph **a. Nuclear** is deleted and replaced with the following:

**a. Nuclear, Biological or Chemical Hazard**

- (1) Nuclear detonation, radiation or reaction; or radioactive contamination.
- (2) The deliberate, unlawful use or threatened use of any biological, chemical or radioactive agent, material, device or weapon.
- (3) Any actions taken to hinder, defend against or respond to (1) or (2) above.

G. The following is added to Section **B. EXCLUSIONS**, item **1. General Exclusions**:

**U.S. Economic or Trade Sanctions**

Any violation of U.S. economic or trade sanctions.

H. Section **B. EXCLUSIONS**, item **2. General Exclusions Not Applicable to Coverage 2 – Identity Recovery**, paragraphs **f.**, **k.**, and **p.** are deleted and replaced with the following:

**f. Government Organizations**

Any “loss” or “claim” based upon, attributable to or arising out of, or brought by or on behalf of any federal, state or local government agency or professional or trade licensing organizations or the enforcement of any governmental law, ordinance, regulation or rule; however, this exclusion shall not apply to:

- (1) Actions or proceedings brought by a governmental authority or regulatory agency acting solely in its capacity as a customer of the “named insured” or a “subsidiary”;

- (2) "Regulatory proceedings" insured under Coverage 5 – Data Compromise Liability; or
- (3) Any fine or penalty imposed by law which arises from a covered "personal data compromise".

**k. Pollution and Contamination**

Any "loss" or liability arising out of "pollutants and contaminants" or the presence of or the actual, alleged or threatened discharge, dispersal, release or escape of "pollutants and contaminants", or any direction or request to test for, monitor, clean up, remove, contain, treat, detoxify or neutralize "pollutants and contaminants", or in any way respond to or assess the effects of "pollutants and contaminants".

**p. Property Damage or Bodily Injury**

"Property damage" or "bodily injury" other than mental anguish or mental injury alleged in a "claim" covered under Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability or Coverage 7 – Electronic Media Liability.

- I. Section **C. LIMITS OF INSURANCE**, item **3. Coverage Sublimits**, paragraph c. is deleted and replaced with the following:

**c. Coverage 3 Sublimits**

The most we will pay under Coverage 3 – Computer Attack for Data Re-Creation, Loss of Business and Crisis Management coverages for "loss" arising from any one "computer attack" is the applicable sublimit for each of those coverages shown in the Declarations. These sublimits are part of, and not in addition to, the aggregate limit for Coverage 3 – Computer Attack shown in the Declarations. The most we will pay under Coverage 3 – Computer Attack for Contingent Loss of Business coverage for "loss" arising from any one "computer attack" is the Contingent Loss of Business sublimit shown in the Declarations. The sublimit for Contingent Loss of Business is part of, and not in addition to, the Loss of Business Sublimit shown in the Declarations.

- J. The following is added to Section **C. LIMITS OF INSURANCE** item **3. Coverage Sublimits**:

**Coverage 8 Sublimits**

The most we will pay under Coverage 8 – Misdirected Payment Fraud for Computer Fraud coverage for "loss" arising from any one "computer fraud event" is the applicable sublimit for that coverage shown in the Declarations. This sublimit is part of, and not in addition to, the aggregate limit for Coverage 8 – Misdirected Payment Fraud shown in the Declarations.

- K. Section **C. LIMITS OF INSURANCE**, item **4. Application of Limits**, paragraph a. is deleted and replaced with the following:

- a. A "computer attack", "cyber extortion threat", "personal data compromise", "identity theft", "wrongful transfer event", "computer fraud event", or "reward payment qualifying event" may be first discovered by you in one "coverage term" but it may cause insured "loss" in one or more subsequent "coverage terms". If so, all insured "loss" arising from such "computer attack", "cyber extortion threat", "personal data compromise", "identity theft", "wrongful transfer event", "computer fraud event", or "reward payment qualifying event" will be subject to the limit of insurance applicable to the "coverage term" when the "computer attack", "cyber extortion threat", "personal data compromise", "identity theft", "wrongful transfer event", "computer fraud event", or "reward payment qualifying event" was first discovered by you.

- L. Section **D. DEDUCTIBLES**, item 2., paragraph a. is deleted and replaced with the following:

- a. "Loss" arising from the same insured event or "interrelated" insured events under Coverage 1 – Data Compromise Response Expenses, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud or Reward Payment Reimbursement coverage.

- M. Section **E. DEFENSE AND SETTLEMENT**, paragraph 2., is deleted and replaced with the following:

2. We may, with your written consent, make any settlement of a “claim” or “regulatory proceeding” which we deem reasonable. If you refuse to consent to any settlement recommended by us and acceptable to the claimant or plaintiff, our liability for all “settlement costs” and “defense costs” resulting from such “claim” or “regulatory proceeding” will not exceed the following:
    - a. the amount for which we could have settled such “claim” or “regulatory proceeding” plus “defense costs” incurred as of the date we proposed such settlement in writing to you; plus
    - b. 80% of any “settlement costs” and “defense costs” incurred after the date of such proposed settlement.
- N. Section **G. ADDITIONAL CONDITIONS**, item **4. Duties in the Event of a Claim, Regulatory Proceeding or Loss**, paragraph c. is deleted and replaced with the following:
- c. In the event of a “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “computer fraud event” insured under Coverage 1– Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud or Computer Fraud coverage, you and any involved “identity recovery insured” must see that the following are done:
    - (1) Notify the police if a law may have been broken.
    - (2) Notify us as soon as possible, but in no event more than 60 days after the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “computer fraud event”. Include a description of any property involved.
    - (3) As soon as possible, give us a description of how, when and where the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “computer fraud event” occurred.
    - (4) As often as may be reasonably required, permit us to:
      - (a) Inspect the property producing the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “computer fraud event”;
      - (b) Examine your books, records, electronic media and records and hardware;
      - (c) Take samples of damaged and undamaged property for inspection, testing and analysis; and
      - (d) Make copies from your books, records, electronic media and records and hardware.
    - (5) Send us signed, sworn proof of “loss” containing the information we request to investigate the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “computer fraud event”. You must do this within 60 days after our request. We will supply you with the necessary forms.
    - (6) Cooperate with us in the investigation or settlement of the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “computer fraud event”.
    - (7) If you intend to continue your business, you must resume all or part of your operations as quickly as possible.
    - (8) Make no statement that will assume any obligation or admit any liability, for any “loss” for which we may be liable, without our prior written consent.
    - (9) Promptly send us any legal papers or notices received concerning the “loss”.

O. The following is added to Section **G. ADDITIONAL CONDITIONS**:

**Additional Policy Protection**

We may, from time to time, offer or arrange to provide benefits specific to one of our risk management benefits which include but are not limited to devices, equipment, services or benefits provided by either us or a third party vendor selected by us. These services or products are designed to mitigate loss, provide loss control, assess risk, identify sources of risk, or develop strategies for eliminating or reducing risk. The benefits are intended to enhance the safety, value, usability, life or protection of you or your insurable assets. Such products or services must be provided by us or by a third party vendor that has an agreement or contract with us. We do not warrant the merchantability, fitness, or quality of any product or service offered or provided by that organization.

P. The following is added to Section **G. ADDITIONAL CONDITIONS**:

**Valuation**

We will determine the value of “money”, “securities”, cryptocurrency and tangible property as follows:

- a. Our payment for loss of “money” or loss payable in “money” will be, at your option, in the “money” of the country in which the “computer fraud event”, “cyber extortion threat”, “reward payments”, or “wrongful transfer event” took place or in the United States of America dollar equivalent thereof determined at the rate of exchange published by the Wall Street Journal at the time of payment of such “loss”.
- b. Our payment for loss of “securities” will be their value at the close of business on the day the “computer fraud event” or the “wrongful transfer event” was discovered, or the day the “securities” were transferred by you in response to the “cyber extortion threat”. At our option, we may:
  - (1) Pay the value of such “securities” to you or replace them in kind, in which event you must assign to us all of your rights, title and interest in those “securities”; or
  - (2) Pay the cost of any Lost Securities Bond required in connection with issuing duplicates of the “securities”; provided that we will be liable only for the cost of the Lost Securities Bond as would be charged for a bond having a penalty not exceeding the lesser of the value of the “securities” at the close of business on the day the “computer fraud event”, “cyber extortion threat” or “wrongful transfer event” was discovered.
- c. Our payment of cryptocurrency will be its value at the close of business on the day the cryptocurrency was transferred by you in response to the covered “cyber extortion threat”.
- d. Our payment for the loss of tangible property will be the smallest of:
  - (1) The cost to replace the tangible property; or
  - (2) The amount you actually spend that is necessary to replace the tangible property.

We will not pay you on a replacement costs basis for any loss of tangible property until such property is actually replaced, unless the replacement is made as soon as reasonably possible after the “loss”. If the lost property is not replaced as soon as reasonably possible after the “loss”, we will pay you the actual cash value of the tangible property on the day the “computer fraud event”, “cyber extortion threat” or “wrongful transfer event” was discovered.

Q. Section **H. DEFINITIONS**, items **5.**, **11.**, **18.**, **24.**, and **34.** are deleted and replaced with the following:

- 5. “Business Income and Extra Expense Loss”** means the loss of Business Income and Extra Expense actually incurred during the Period of Restoration.
  - a. As used in this definition, Business Income means the sum of:
    - (1) Net income (net profit or loss before income taxes) that would have been earned or incurred; and
    - (2) Continuing normal and necessary operating expenses incurred, including “employee” and “executive” payroll.
  - b. As used in this definition, Extra Expense means the additional cost you incur to operate your business over and above the cost that you normally would have incurred to operate your business during the same period had no “computer attack” occurred.
  - c. As used in this definition, Period of Restoration means the period of time that begins after the “waiting period” and continues until the earlier of:
    - (1) The date that all data restoration, data re-creation and system restoration directly related to the “computer attack” has been completed;
    - (2) The date on which such data restoration, data re-creation and system restoration could have been completed with the exercise of due diligence and dispatch; or
    - (3) The “maximum period of restoration” has elapsed.
- 11. “Cyber Extortion Expenses”** means:
  - a. The cost of a negotiator or investigator retained by you in connection with a “cyber extortion threat”; and

- b. Any amount paid by you in response to a “cyber extortion threat” to the party that made the “cyber extortion threat” for the purposes of eliminating the “cyber extortion threat” when such expenses are necessary and reasonable and arise directly from a “cyber extortion threat”. This includes any payment made in the form of “money”, “securities”, cryptocurrency (including, but not limited to, Bitcoin, Ethereum and other forms of digital, virtual or electronic currency) or tangible goods. The payment of “cyber extortion expenses” must be approved in advance by us. We will not unreasonably withhold our approval. However, we may pay for “cyber extortion expenses” that were not approved in advance by us if we determine the following:
- (1) It was not practical for you to obtain our prior approval; and
  - (2) If consulted at the time, we would have approved the payment.

At our sole discretion, we may choose to pay “cyber extortion expenses” in excess of the limit shown in the Declarations if doing so reduces the total amount of “loss” payable under this Cyber Risk Coverage.

**18. “Employee”** means any natural person, other than an “executive”, who was, now is or will be:

- a. Employed on a full-time or part-time basis by you;
- 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 b.;
- d. Your volunteer worker, which includes unpaid interns; or
- e. An “independent contractor”.

**24. “Insured”** means:

- a. With respect to Coverage 1 – Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud, Computer Fraud coverage, and Reward Payment Reimbursement coverage, “insured” means a named insured;
- b. With respect to Coverage 5 – Data Compromise Liability, Coverage 6 – Network Security Liability and Coverage 7 – Electronic Media Liability, “insured” means:
  - (1) Any “named insured”; and
  - (2) Any “employee” or “executive” of a “named insured”, but:
    - (a) Only for the conduct of the “named insured’s” business within the scope of his or her employment or duties as an “employee” or “executive”; and
    - (b) Such “employee” or “executive” will not be an “insured” to the extent his or her actions or omissions are criminal, fraudulent, dishonest or constitute an intentional or knowing violation of the law.

**34. “Pollutants and contaminants”** include, but are not limited to, any solid, liquid, gaseous, biological, radiological or thermal irritant or contaminant, including smoke, vapor, dust, fibers, mold, spores, fungi, microorganism, virus, diseases, germs, soot, fumes, asbestos, acids, alkalis, chemicals, and waste. Waste includes, but is not limited to, materials to be recycled, reconditioned or reclaimed and nuclear materials.

R. Section H. **DEFINITIONS**, item 10. “**Coverage Territory**”, paragraph a. is deleted and replaced with the following:

- a. With respect to Coverage 1 – Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud, Computer Fraud coverage, and Reward Payment Reimbursement coverage, “coverage territory” means anywhere in the world.

- S. Section **H. DEFINITIONS**, item **30. “Personal Data Compromise”**, paragraph a.(1) is deleted and replaced with the following:
- (1) You, including “personally identifying information” or “personally sensitive information” residing on a personal device owned or leased by one of your “employees” or “executives” as long as such information was residing on such device with your authorization; or
- T. Section **H. DEFINITIONS**, item **45. “Wrongful transfer event”**, paragraph a. is deleted and replaced with the following:
- a. “Wrongful transfer event” means an intentional and criminal deception of an “insured” or a financial institution with which the “insured” has an account. The deception must be perpetrated by a person who is not an “employee”, using email, facsimile or telephone communications to induce the “insured” or the financial institution to send or divert “money”, “securities” or tangible property. The deception must result in direct financial loss to an “insured”.
- U. The following is added to Section **H. DEFINITIONS**, item **26. “Loss”**:
- With respect to Computer Fraud coverage, “loss” means “computer fraud costs”, and with respect to Reward Payment Reimbursement coverage, “loss” means “reward payments”.
- V. The following is added to Section **H. DEFINITIONS**, item **39. “System Restoration Costs”**:
- At our sole discretion, we may choose to pay to repair or replace hardware if doing so reduces the amount of “loss” payable under this Coverage Part.
- W. The following are added to Section **H. DEFINITIONS**:
- “Computer fraud costs”**
- a. “Computer fraud costs” means the amount of fraudulent obtained from the insured. “Computer fraud costs” include the direct financial loss on .
  - b. “Computer fraud costs” do not include any of the following:
    - (1) Other expenses that arise from the “computer fraud event”;
    - (2) Indirect loss, such as “bodily injury”, lost time, lost wages, identity recovery expenses or damaged reputation;
    - (3) Any interest, time value or potential investment gain on the amount of financial loss; or
    - (4) Any portion of such amount that has been or can reasonably be expected to be reimbursed by a third party, such as a financial institution.
- “Computer fraud event”**
- a. “Computer fraud event” means an “unauthorized access incident” that leads to the intentional, unauthorized and fraudulent entry of or change to data or instructions within your “computer system”. Such fraudulent entry or change must be conducted by a person who is not an “employee” or “executive”. Such fraudulent entry or change must cause “money”, “securities” or tangible property to be sent or diverted. The fraudulent entry or change must result in direct financial loss to an “insured”.
  - b. “Computer fraud event” does not mean or include any occurrence:
    - (1) In which the “insured” is threatened or coerced to send money or divert a payment; or
    - (2) Arising from a dispute or a disagreement over the completeness, authenticity or value of a product, a service or a financial instrument.
- “Independent Contractor”** means a natural person who provides goods or services to the “named insured” under terms specified in a written contract, but only while acting on behalf of, at the direction of, and under the supervision of the “named insured”.



**“Maximum period of restoration”** means the period of time beginning with the date the “business income and extra expense loss” is discovered by you and continues for the number of days shown in the Declarations.

**“Money”**

- a. “Money” means a medium of exchange in current use and authorized or adopted by a domestic or foreign government, including currency, coins, banknotes, bullion, travelers’ checks, registered checks and money orders held for sale to the public.
- b. “Money” does not mean or include any cryptocurrency, whether or not authorized or adopted by a domestic or foreign government. Cryptocurrency includes, but is not limited to, Bitcoin, Ethereum and other forms of digital, virtual or electronic currency.

**“Reward Payments”** means an amount of “money” paid by you to any individual(s) for information regarding a “reward payment qualifying event”. Such individual may not be:

- (1) You;
- (2) Your “employee”;
- (3) Anyone hired by you to investigate a “reward qualifying event”; or
- (4) A member of law enforcement.

**“Reward Payment Qualifying Event”** means a “personal data compromise”, “computer attack”, “cyber extortion threat”, “computer fraud event” or “wrongful transfer event”.

**“Securities”**

- a. “Securities” means:
  - (1) Written negotiable and non-negotiable instruments or contracts representing “money” or tangible property; or
  - (2) Uncertified securities
- b. “Securities” does not mean or include “money”.

**“Waiting period”** means the period of time that begins once the “business income and extra expense loss” is discovered by you, and ends once the number of hours shown in the Declarations has elapsed. The “business income waiting period” does not apply to Extra Expense.

ALL OTHER PROVISIONS OF THIS POLICY APPLY.

Named Insured: Sample Policy				
Policy Number: 01-CY-0005511657-00	Transaction Effective Date: 10/01/2021	Policy Period: 10/01/2021 to 10/01/2022	Issue Date: 09/17/2021	Ref. No.: N/A

## Invoice Manipulation Fraud

This endorsement changes the policy. Please read it carefully.

This endorsement modifies insurance provided under the following:

### Cyber Risk Coverage Form

A. The following is added to Section **A. COVERAGE**, item **8. Misdirected Payment Fraud**:

#### Invoice Manipulation Fraud

a. This Invoice Manipulation Fraud coverage applies only if all of the following conditions are met:

- (1) There has been an "invoice manipulation fraud event" against you; and
- (2) Such "invoice manipulation fraud event" took place in the "coverage territory"; and
- (3) Such "invoice manipulation fraud event" is first discovered by you during the "coverage term"; and
- (4) Such "invoice manipulation fraud event" is reported to us within 60 days after the date it is first discovered by you; and
- (5) Such "invoice manipulation fraud event" is reported in writing by you to the police; and
- (6) As a result of such "invoice manipulation fraud event", there have been "invoice manipulation fraud costs".

b. If the conditions listed in a. above have been met, then we will pay your necessary and reasonable "invoice manipulation fraud costs" arising directly from the "invoice manipulation fraud event".

B. The following is added to Section **C. LIMITS OF INSURANCE**, item **3. Coverage Sublimits**:

#### Coverage 8 Sublimits

The most we will pay under Coverage 8 – Misdirected Payment Fraud for Invoice Manipulation Fraud coverage for "loss" arising from any one "invoice manipulation fraud event" is the applicable sublimit for that coverage shown in the Declarations. This sublimit is part of, and not in addition to, the aggregate limit for Coverage 8 – Misdirected Payment Fraud shown in the Declarations.

C. Section **C. LIMITS OF INSURANCE**, item **4. Application of Limits**, paragraph a. is deleted and replaced with the following:

- a. A "computer attack", "cyber extortion threat", "personal data compromise", "identity theft", "wrongful transfer event", or "invoice manipulation fraud event" may be first discovered by you in one "coverage term" but it may cause insured "loss" in one or more subsequent "coverage terms". If so, all insured "loss" arising from such "computer attack", "cyber extortion threat", "personal data compromise", "identity theft", "wrongful transfer event", or "invoice manipulation fraud event" will be subject to the limit of insurance applicable to the "coverage term" when the "computer attack", "cyber extortion threat", "personal data compromise", "identity theft", "wrongful transfer event", or "invoice manipulation fraud event" was first discovered by you.

D. Section **G. ADDITIONAL CONDITIONS**, item **4. Duties in the Event of a Claim, Regulatory Proceeding or Loss**, paragraph c. is deleted and replaced with the following:

- c. In the event of a “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “invoice manipulation fraud event” insured under Coverage 1– Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud or Invoice Manipulation Fraud coverage, you and any involved “identity recovery insured” must see that the following are done:
- (1) Notify the police if a law may have been broken.
  - (2) Notify us as soon as possible, but in no event more than 60 days after the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “invoice manipulation fraud event”. Include a description of any property involved.
  - (3) As soon as possible, give us a description of how, when and where the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “invoice manipulation fraud event” occurred.
  - (4) As often as may be reasonably required, permit us to:
    - (a) Inspect the property proving the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “invoice manipulation fraud event”;
    - (b) Examine your books, records, electronic media and records and hardware;
    - (c) Take samples of damaged and undamaged property for inspection, testing and analysis; and
    - (d) Make copies from your books, records, electronic media and records and hardware.
  - (5) Send us signed sworn proof of “loss” containing the information we request to investigate the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “invoice manipulation fraud event”. You must do this within 60 days after our request. We will supply you with the necessary forms.
  - (6) Cooperate with us in the investigation or settlement of the “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat”, “wrongful transfer event” or “invoice manipulation fraud event”.
  - (7) If you intend to continue your business, you must resume all or part of your operations as quickly as possible.
  - (8) Make no statement that will assume any obligation or admit any liability, for any “loss” for which we may be liable, without our prior written consent.
  - (9) Promptly send us any legal papers or notices received concerning the “loss”.

E. With respect to the coverage provided by this Invoice Manipulation Fraud endorsement only, the following is added to Section **G. ADDITIONAL CONDITIONS**:

**Valuation**

We will determine the value of “money”, “securities”, and tangible property as follows:

- a. Our payment for loss of “money” or loss payable in “money” will be, at your option, in the “money” of the country in which the “invoice manipulation fraud event” took place or in the United States of America dollar equivalent thereof determined at the rate of exchange published by the Wall Street Journal at the time of payment of such “loss”.
- b. Our payment for loss of “securities” will be their value at the close of business on the day the “invoice manipulation fraud event” was discovered. At our option, we may:
  - (1) Pay the value of such “securities” to you or replace them in kind, in which event you must assign to us all of your rights, title and interest in those “securities”; or
  - (2) Pay the cost of any Lost Securities Bond required in connection with issuing duplicates of the “securities”; provided that we will be liable only for the cost of the Lost Securities Bond as would be

charged for a bond having a penalty not exceeding the lesser of the value of the “securities” at the close of business on the day the “invoice manipulation fraud event” was discovered.

- c. Our payment for the loss of tangible property will be the smallest of:
- (1) The cost to replace the tangible property; or
  - (2) The amount you actually spend that is necessary to replace the tangible property.

We will not pay you on a replacement costs basis for any loss of tangible property until such property is actually replaced and unless the replacement is made as soon as reasonably possible after the “loss”. If the lost property is not replaced as soon as reasonably possible after the “loss”, we will pay you the actual cash value of the tangible property on the day the “invoice manipulation fraud event” was discovered.

F. Section **H. DEFINITIONS**, item **10. “Coverage Territory”**, paragraph a. is deleted and replaced with the following:

- a. With respect to Coverage 1 – Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud, and Invoice Manipulation Fraud coverage, “coverage territory” means anywhere in the world.

G. Section **H. DEFINITIONS**, item **24. “Insured”**, paragraph a. is deleted and replaced with the following:

- a. With respect to Coverage 1 – Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud, and Invoice Manipulation Fraud coverage, “insured” means any “named insured”.

H. The following is added to Section **H. DEFINITIONS**, item **26. “Loss”**:

With respect to Invoice Manipulation Fraud coverage, “loss” means “invoice manipulation fraud costs”.

I. The following are added to Section **H. DEFINITIONS**:

**“Independent Contractor”** means a natural person who provides goods or services to the “named insured” under terms specified in a written contract, but only while acting on behalf of, at the direction of, and under the supervision of the “named insured”.

**“Invoice manipulation fraud costs”**

- a. “Invoice manipulation fraud costs” means the amount an “insured” is unable to obtain for goods or services provided by the “insured” to a third party.
- b. “Invoice manipulation fraud costs” do not include any of the following:
- (1) Other expenses that arise from the “invoice manipulation fraud event”;
  - (2) Indirect loss, such as “bodily injury”, lost time, lost wages, identity recovery expenses or damaged reputation;
  - (3) Any interest, time value or potential investment gain on the amount of financial loss; or
  - (4) Any portion of such amount that has been or can reasonably be expected to be reimbursed by a third party, such as a financial institution.

**“Invoice manipulation fraud event”**

“Invoice manipulation fraud event” means an “unauthorized access incident” that directly leads to the intentional, unauthorized and fraudulent release or distribution of an invoice or other form of payment instructions to a third party. The release or distribution of such invoice or other form of payment instructions must have occurred as a direct result of the “unauthorized access incident”.

- a. An “invoice manipulation fraud event” must be perpetrated on a:

- (1) “Computer system” that is owned or leased by you and operated under your control; or
- (2) Cloud-Based Email Service.
- b. An “invoice manipulation fraud event” must:
  - (1) Be conducted by a person who is not an “employee”, “executive” or “independent contractor”;
  - (2) Cause “money”, “securities” or tangible property to be sent or diverted; and
  - (3) Result in direct financial loss to an “insured”.
- c. “Invoice manipulation fraud event” does not mean or include any occurrence:
  - (1) In which the “insured” is threatened or coerced to send money or divert a payment; or
  - (2) Arising from a dispute or a disagreement over the completeness, authenticity or value of a product, a service or a financial instrument.
- d. For purposes of this definition, Cloud-Based Email Service means a hosted subscription service that you use (pursuant to a written contract with the service provider) to conduct business via tools such as email, shared calendars, online file storage and instant messaging.

**“Money”**

- a. “Money” means a medium of exchange in current use and authorized or adopted by a domestic or foreign government, including currency, coins, banknotes, bullion, travelers’ checks, registered checks and money orders held for sale to the public.
- b. “Money” does not mean or include any cryptocurrency, whether or not authorized or adopted by a domestic or foreign government. Cryptocurrency includes, but is not limited to, Bitcoin, Ethereum and other forms of digital, virtual or electronic currency.

**“Securities”**

- a. “Securities” means:
  - (1) Written negotiable and non-negotiable instrument or contract representing “money” or tangible property; or
  - (2) Uncertified securities.
- b. “Securities” does not mean or include “money”.

ALL OTHER PROVISIONS OF THIS POLICY APPLY.

Named Insured: Sample Policy				
Policy Number: 01-CY-0005511657-00	Transaction Effective Date: 10/01/2021	Policy Period: 10/01/2021 to 10/01/2022	Issue Date: 09/17/2021	Ref. No.: N/A

## PCI Assessments, Fines and Penalties

This endorsement changes the policy. Please read it carefully.

This endorsement modifies insurance provided under the following:

**Cyber Risk Coverage Form**

Section **A. COVERAGE**, item **1. Data Compromise Response Expenses**, paragraph b. **(7) PCI Fines and Penalties** is deleted and replaced with the following:

**(7) PCI Fines and Penalties**

Payment Card Industry assessments, fines and penalties imposed on you under a contract to which you are a party.

This does not include any:

- (a) Increased transaction costs;
- (b) Any assessments, fines and penalties not imposed for a covered "personal data compromise";
- (c) Interchange fees;
- (d) Chargebacks;
- (e) Subsequent assessments, fines and penalties imposed due to continued PCI non-compliance; or
- (f) Any portion of such amount that has been or can reasonably be expected to be reimbursed by a third party, such as a financial institution.

ALL OTHER PROVISIONS OF THIS POLICY APPLY.

Named Insured: Sample Policy				
Policy Number: 01-CY-0005511657-00	Transaction Effective Date: 10/01/2021	Policy Period: 10/01/2021 to 10/01/2022	Issue Date: 09/17/2021	Ref. No.: N/A

## Reputational Harm

This endorsement changes the policy. Please read it carefully.

This endorsement modifies insurance provided under the following:

### Cyber Risk Coverage Form

A. The following is added to Section **A. COVERAGE**:

#### Reputational Harm

- a. This Reputational Harm coverage applies only if there has been a “personal data compromise” for which you provided notifications and services to “affected individuals” in consultation with us pursuant to Coverage 1 – Data Compromise Response Expenses.
- b. If the conditions listed in a. above have been met, then we will pay your necessary and reasonable “reputational harm costs” incurred during the “period of indemnification” and arising directly from the “personal data compromise”.

B. Section **D. DEDUCTIBLES**, item 2, paragraph a. is deleted and replaced with the following:

- a. “Loss” arising from the same insured event or “interrelated” insured events under Coverage 1 – Data Compromise Response Expenses, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud or Reputational Harm coverage.

C. Section **G. ADDITIONAL CONDITIONS**, item 4. **Duties in the Event of a Claim, Regulatory Proceeding or Loss**, paragraph c., first paragraph, is deleted and replaced with the following:

- c. In the event of a “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat” or “wrongful transfer event” insured under Coverage 1– Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud or Reputational Harm coverage, you and any involved “identity recovery insured” must see that the following are done:

D. The following are added to Section **H. DEFINITIONS**:

“**Period of indemnification**” means the period of time that begins on the date you first provided notification to “affected individuals” pursuant to Coverage 1 – Data Compromise Response Expenses and ends after the number of days shown in the Declarations.

#### “Reputational harm costs”

- a. “Reputational harm costs” means the loss of Business Income during the “period of indemnification” arising directly from damage to your reputation caused by a “personal data compromise”.

As used in this definition, Business Income means the sum of:

- (1) Net income (net profit or loss before income taxes) that would have been earned or incurred; and

© 2020, The Hartford Steam Boiler Inspection and Insurance Company. All rights reserved.

- (2) Continuing normal and necessary operating expenses incurred, including “employee” and “executive” payroll.
- b. “Reputational harm costs” does not mean or include Business Income you lose due to:
- (1) Unfavorable or deteriorated business conditions;
  - (2) Decreased market share;
  - (3) Any other consequential damages or losses;
  - (4) Legal costs or expenses;
  - (5) Investment income;
  - (6) Bank interest;
  - (7) Seasonal fluctuations;
  - (8) Additional costs you incur to operate your business over and above the costs that you normally would have incurred to operate your business during the same period had no “personal data compromise” occurred.
- E. Section **H. DEFINITIONS**, item **10. “Coverage Territory”**, paragraph a. is deleted and replaced with the following:
- a. With respect to Coverage 1 – Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud and Reputational Harm coverage, “coverage territory” means anywhere in the world.
- F. Section **H. DEFINITIONS**, item **24. “Insured”**, paragraph a. is deleted and replaced with the following:
- a. With respect to Coverage 1 – Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud and Reputational Harm coverage, “insured” means any “named insured”.
- G. The following is added to Section **H. DEFINITIONS**, item **23. “Loss”**:
- With respect to Reputational Harm coverage, “loss” means “reputational harm costs”.

ALL OTHER PROVISIONS OF THIS POLICY APPLY.



Named Insured: Sample Policy				
Policy Number: 01-CY-0005511657-00	Transaction Effective Date: 10/01/2021	Policy Period: 10/01/2021 to 10/01/2022	Issue Date: 09/17/2021	Ref. No.: N/A

## Telecommunications Fraud

This endorsement changes the policy. Please read it carefully.

This endorsement modifies insurance provided under the following:

### Cyber Risk Coverage Form

A. The following is added to Section **A. COVERAGE**:

#### Telecommunications Fraud

- a. This Telecommunications Fraud coverage applies only if all of the following conditions are met:
- (1) There has been a “computer attack” on a “telecommunications system” that is owned or leased by you and operated under your control; and
  - (2) Such “computer attack” took place in the “coverage territory”; and
  - (3) Such “computer attack” is first discovered by you during the “coverage term”; and
  - (4) Such “computer attack” is reported to us within 60 days after the date it is first discovered by you; and
  - (5) Such “computer attack” is reported in writing by you to the police; and
  - (6) As a result of such “computer attack” there have been “telecommunications fraud costs”.
- b. If the conditions listed in a. above have been met, then we will pay your necessary and reasonable “telecommunications fraud costs” arising directly from the “computer attack”.

B. Section **D. DEDUCTIBLES**, item 2., paragraph a. is deleted and replaced with the following:

- a. “Loss arising from the same insured event or “interrelated” insured events under Coverage 1 – Data Compromise Response Expenses, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud or Telecommunications Fraud coverage.

C. Section **G. ADDITIONAL CONDITIONS**, item 4. **Duties in the Event of a Claim, Regulatory Proceeding or Loss**, paragraph c., first paragraph, is deleted and replaced with the following:

- c. In the event of a “personal data compromise”, “identity theft”, “computer attack”, “cyber extortion threat” or “wrongful transfer event” insured under Coverage 1– Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud or Telecommunications Fraud coverage, you and any involved “identity recovery insured” must see that the following are done:

D. The following are added to section **H. DEFINITIONS**:

“**Telecommunications fraud costs**” means any payment that you are responsible for making to your Telephone Service Provider as a result of a “computer attack” on a “telecommunications system” that is owned or leased by you and operated under your control. As used in this definition, Telephone Service Provider means a business with which you have a written contract to provide you with telephone services.

© 2020, The Hartford Steam Boiler Inspection and Insurance Company. All rights reserved.

“**Telecommunications system**” means any telephone, fax network or system that is owned or leased by you and operated under your control.

- E. Section **H. DEFINITIONS**, item **10. “Coverage Territory”**, paragraph a. is deleted and replaced with the following:
- a. With respect to Coverage 1 – Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud, and Telecommunications Fraud coverage, “coverage territory” means anywhere in the world.
- F. Section **H. DEFINITIONS**, item **24. “Insured”**, paragraph a. is deleted and replaced with the following:
- a. With respect to Coverage 1 – Data Compromise Response Expenses, Coverage 2 – Identity Recovery, Coverage 3 – Computer Attack, Coverage 4 – Cyber Extortion, Coverage 8 – Misdirected Payment Fraud, and Telecommunications Fraud coverage, “insured” means any “named insured”.
- G. The following is added to Section **H. DEFINITIONS**, item **26. “Loss”**:

With respect to Telecommunications Fraud coverage, “loss” means “telecommunications fraud costs”.

ALL OTHER PROVISIONS OF THIS POLICY APPLY.

Sample



Named Insured: Sample Policy				
Policy Number: 01-CY-0005511657-00	Transaction Effective Date: 10/01/2021	Policy Period: 10/01/2021to 10/01/2022	Issue Date: 09/17/2021	Ref. No.: N/A

**Terrorism Risk Insurance Act Disclosure**

This endorsement is attached to and made part of your policy in response to the disclosure requirements of the Terrorism Risk Insurance Act, as amended.

This endorsement modifies insurance provided under the following:  
**Cyber Risk Coverage Form**

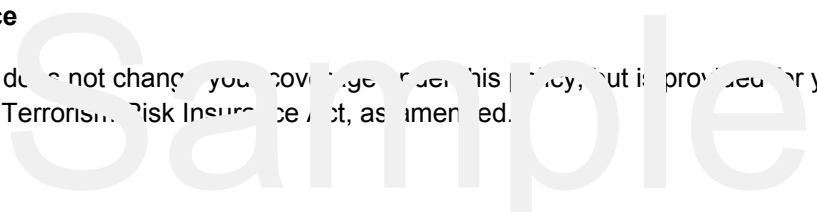
**NOTICE OF TERRORISM INSURANCE COVERAGE**

**Applicable Premium**

The portion of your annual premium that is attributable to coverage for acts of terrorism is \$0, and does not include any charges for the portion of losses covered by the United States government under the Act.

**Informational Notice**

The following notice does not change your coverage under this policy, but is provided for your information in compliance with the Terrorism Risk Insurance Act, as amended.



Coverage for acts of terrorism is included in your policy. You are hereby notified that the Terrorism Risk Insurance Act, as amended in 2019, defines an act of terrorism 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. Under your coverage, 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.