ENDORSEMENT NO.

CYBER SUITE COVERAGE ENDORSEMENT

This Endorsement, effective at 12:01 a.m. on , forms part of

Policy No.
Issued to
Issued by: The Hartford Steam Boiler Inspection and Insurance Company

This endorsement modifies insurance provided under the following:

Professional and Business Liability Policy

Throughout this Coverage Endorsement (hereinafter referred to as "Cyber Coverage"), the words "you" and "your" refer to the Named Insured(s) shown in the Cyber Suite Supplemental Declarations of this Cyber Coverage and any other person(s) or organization(s) qualifying as a Named Insured under this Cyber Coverage. The words "we", "us" and "our" refer to the company providing this insurance.

Other words and phrases that appear in quotations have special meaning, specifically applicable to this endorsement. Refer to **DEFINITIONS**. Any definitions contained in any other coverage provided under this policy do not apply to this endorsement, unless specifically stated otherwise in an endorsement(s) attached hereto.

The terms and conditions of Section **X. CANCELLATION** or Section **XI. CANCELLATION**, as applicable, and any amendment to such terms incorporated by endorsement are hereby incorporated herein and shall apply to coverage as is afforded by this Cyber Coverage, unless specifically stated otherwise in an endorsement(s) attached hereto.

A. COVERAGE

This section lists the coverages that apply only if indicated in the Cyber Suite Supplemental Declarations.

1. Data Compromise Response Expenses

a. 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 "policy period"; and

(4) Such "personal data compromise" 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 coverage for the following expenses when they arise directly from such "personal data compromise" 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

We will pay for a 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

We will pay for a 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) Public Relations

We will pay for a professional public relations firm review of and response to the potential impact of the "personal data compromise" on your business relationships.

This includes necessary and reasonable costs to implement public relations recommendations of such firm. This may include advertising and special promotions

designed to retain your relationship with "affected individuals". However, we will not pay for:

(a) Promotions provided to any of your directors or employees; or

(b) Promotion costs exceeding $25 per "affected individual".

(6) Regulatory Fines and Penalties

We will pay for 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

We will pay for 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. Computer Attack

a. 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 "policy period"; 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".

(5) Public Relations

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.

3. Cyber Extortion

a. 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 "policy period"; 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 for your necessary and reasonable "cyber extortion expenses" arising directly from such "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.

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

4. Data Compromise Liability

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

(1) During the "policy period" or any applicable Extended Reporting Period, you first receive notice of one of the following:

(a) A "claim" brought by or on behalf of one or more "affected individuals"; 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 during the "coverage term";

(b) Took place in the "coverage territory"; and

(c) Was submitted to us and insured under 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 your behalf any covered:

(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.

5. Network Security Liability

a. Network Security Liability applies only if all of the following conditions are met:

(1) During the "policy period" or any applicable Extended Reporting Period, you first receive notice of a "claim" which arises from a "network security incident" that:

(a) Took place during the "coverage term"; 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 your behalf any covered "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.

6. Electronic Media Liability

a. Electronic Media Liability applies only if all of the following conditions are met:

(1) During the "policy period" or any applicable Extended Reporting Period, you first receive notice of a "claim" which arises from an "electronic media incident" that:

(a) Took place during the "coverage term"; 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 your behalf any covered "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.

7. Identity Recovery

a. 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 Cyber Coverage; 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 "policy period"; 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

We will pay for the services of an "identity recovery case manager" as needed to respond to the "identity theft"; and

(2) Expense Reimbursement

We will pay for reimbursement of necessary and reasonable "identity recovery expenses" incurred as a direct result of the "identity theft".

B. EXCLUSIONS

The following additional exclusions apply to the coverage provided by this endorsement:

We will not pay for costs or "loss" arising from, based upon, or alleging the following:

1. Nuclear reaction or radiation or radioactive contamination, however caused.

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

a. War, including undeclared or civil war;

b. 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

c. Insurrection, rebellion, revolution, usurped power, political violence or action taken by governmental authority in hindering or defending against any of these.

3. Failure or interruption of or damage to the internet or an internet service provider.

4. Any attack on, incident involving, or loss to any computer or system of computers that is not a "computer system".

5. Costs to research or correct any deficiency.

6. Any fines or penalties other than those explicitly covered under Data Compromise Response Expenses.

7. Any criminal investigations or proceedings.

8. Your intentional or willful complicity in a covered "loss" event.

9. Your reckless disregard for the security of your "computer system" or data, including confidential or sensitive information of others in your care, custody or control.

10. Any criminal, fraudulent, malicious or dishonest act, error or omission, or any intentional or knowing violation of any statute, rule or law by you.

11. Any "personal data compromise", "computer attack", "cyber extortion threat" or "wrongful act" occurring before the "coverage term".

12. 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".

13. 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.

14. Any threat, extortion or blackmail including, but not limited to, ransom payments and private security assistance. Extortion as used in this exclusion is all types of extortion except a "cyber extortion threat" as defined and covered under the Cyber Extortion coverage in this Cyber Coverage.
15. Any oral or written publication of material, if done by you or at your direction with knowledge of its falsity.
16. "Property damage" or "bodily injury" other than mental anguish or mental injury alleged in a "claim" covered under Electronic Media Liability.
17. The theft of a professional or business identity.
18. 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.
19. An "identity theft" that is not reported in writing to the police.

C. LIMITS OF INSURANCE

1. Aggregate Limits

The First Party Aggregate Limit shown in the Cyber Suite Supplemental Declarations is the most we will pay for all "loss" under all the Data Compromise Response Expenses, Computer Attack and Cyber Extortion coverages in any one "policy period". The First Party Aggregate Limit shown in the Cyber Suite Supplemental Declarations applies regardless of the number of insured events first discovered during the "policy period".

Except for post-judgment interest, the Third Party Aggregate Limit shown in the Cyber Suite Supplemental Declarations is the most we will pay for all "loss" under all the Data Compromise Liability, Network Security Liability and Electronic Media Liability coverages in any one "policy period" or any applicable Extended Reporting Period. The Third Party Aggregate Limit shown in the Cyber Suite Supplemental Declarations applies regardless of the number of insured "claims" or "regulatory proceedings" first received during the "policy period" or any applicable Extended Reporting Period.

The Identity Recovery Coverage is subject to the Identity Recovery Limit as shown in the Cyber Suite Supplemental Declarations.

2. Coverage Sublimits

a. Data Compromise Sublimits

The most we will pay under Data Compromise Response Expenses for Forensic IT Review, Legal Review, Public Relations, 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 Cyber Suite Supplemental Declarations.

These sublimits are part of, and not in addition to, the First Party Aggregate Limit shown in the Cyber Suite Supplemental Declarations. Public Relations coverage is also subject to a limit per "affected individual" as described in **A.1.b.(5)**.

b. Computer Attack Sublimits

The most we will pay under Computer Attack for Loss of Business and Public Relations coverages for "loss" arising from any one "computer attack" is the applicable sublimit for each of those coverages shown in the Cyber Suite Supplemental Declarations. These sublimits are part of, and not in addition to, the First Party Aggregate Limit shown in the Cyber Suite Supplemental Declarations.

c. Cyber Extortion Sublimit

The most we will pay under Cyber Extortion coverage for "loss" arising from one "cyber extortion threat" is the applicable sublimit shown in the Cyber Suite Supplemental Declarations. This sublimit is part of, and not in addition to, the First Party Aggregate Limit shown in the Cyber Suite Supplemental Declarations.

d. Identity Recovery Sublimits

The following provisions are applicable only to the Identity Recovery Coverage.

(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 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 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 Cyber Suite Supplemental Declarations. This sublimit is part of, and not in addition to, the aggregate limit for 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 Cyber Suite Supplemental Declarations. This sublimit is part of, and not in addition to, the aggregate limit for 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 Unnamed Costs) of the definition of "identity recovery expenses" is subject to the Miscellaneous Unnamed Costs sublimit shown in the Cyber Suite Supplemental Declarations. This sublimit is part of, and not in addition to, the aggregate limit for Identity Recovery. Coverage is limited to costs incurred within 12 months after the first discovery of the "identity theft" by the "identity recovery insured".

3. Application of Limits

a. A "computer attack", "cyber extortion threat", "personal data compromise" or "identity theft" may be first discovered by you in one "policy period" but it may cause insured "loss" in one or more subsequent "policy periods". If so, all insured "loss" arising from such "computer attack", "cyber extortion threat", "personal data compromise" or "identity theft" will be subject to the limit of insurance applicable to the "policy period" when the "computer attack", "cyber extortion threat", "personal data compromise" or "identity theft" was first discovered by you.

b. You may first receive notice of a "claim" or "regulatory proceeding" in one "policy period" but it may cause insured "loss" in one or more subsequent "policy periods". If so, all insured "loss" arising from such "claim" or "regulatory proceeding" will be subject to the limit of insurance applicable to the "policy period" 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 "policy period".

d. Coverage for Services to Affected Individuals under 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" until the amount of the insured "loss" exceeds the deductible amount shown in the Cyber Suite Supplemental Declarations. We will then pay the amount of "loss" in excess of the applicable deductible amount, subject to the applicable limits shown in the Cyber Suite Supplemental 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 Data Compromise Response Expenses, Computer Attack or Cyber Extortion.

b. "Loss" resulting from the same "wrongful act" or interrelated "wrongful acts" insured under Data Compromise Liability, Network Security Liability or 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 Identity Recovery is not subject to a deductible.

E. ADDITIONAL CONDITIONS

The following conditions apply:

1. Bankruptcy

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

2. Defense And Settlement

a. We shall have the right and the duty to assume the defense of any applicable "claim" or "regulatory proceeding" against you. You shall give us such information and cooperation as we may reasonably require.

b. You shall not admit liability for or settle any "claim" or "regulatory proceeding" or incur any defense costs without our prior written consent.

c. 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.

d. If you refuse to consent to any settlement recommended by us and acceptable to the claimant, we may then withdraw from your defense by tendering control of the defense to you. From that point forward, you shall, at your own expense, negotiate or defend such "claim" or "regulatory proceeding" independently of us. Our liability shall not exceed the amount for which the "claim" or suit could have been settled if such recommendation was consented to, plus "defense costs" incurred by us, and "defense costs" incurred by you with our written consent, prior to the date of such refusal.

e. 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.

f. We will pay all interest on that amount of any judgment within the applicable limit of insurance which accrues:

(1) After entry of judgment; and

(2) 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.

3. Due Diligence

You agree to use due diligence to prevent and mitigate "loss" insured under this Cyber Coverage. 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 "policy period", 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 "policy period"; or

(2) Anytime during the extended reporting periods (if applicable).

b. If a "claim" or "regulatory proceeding" is brought against you, 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".

c. In the event of a "personal data compromise", "computer attack", "cyber extortion threat" or "identity theft", insured under this Cyber 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 practicable, but in no event more than 60 days after the "personal data compromise", "computer attack", "cyber extortion threat" or "identity theft". 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", "computer attack", "cyber extortion threat" or "identity theft" occurred.

(4) As often as may be reasonably required, permit us to:

(a) Inspect the property proving the "personal data compromise", "computer attack", "cyber extortion threat" or "identity theft";

(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", "computer attack", "cyber extortion threat" or "identity theft". 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", "computer attack", "cyber extortion threat" or "identity theft".

(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 you under oath at such times as may be reasonably required, about any matter relating to this insurance or the "claim", "regulatory proceeding" or "loss", including your books and records. In the event of an examination, your answers must be signed.

e. You may not, except at your own cost, voluntarily make a payment, assume any obligation, or incur any expense without our prior written consent.

5. Extended Reporting Periods

a. You will have the right to the Extended Reporting Periods described in this section, in the event of a "termination of coverage".

b. If a "termination of coverage" has occurred, you will have the right to the following:

(1) At no additional premium, an Automatic Extended Reporting Period of 30 days immediately following the effective date of the "termination of coverage" during which you may first receive notice of a "claim" or "regulatory proceeding" arising directly from a "wrongful act" occurring before the end of the "policy period" and which is otherwise insured by this Cyber Coverage; and

(2) 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 effective date of the "termination of coverage" during which you may first receive notice of a "claim" or "regulatory proceeding" arising directly from a "wrongful act" occurring before the end of the "policy period" and which is otherwise insured by this Cyber Coverage.

To obtain the Supplemental Extended Reporting Period, you must request it in writing and pay the additional premium due, within 30 days after the effective date of "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.

This insurance, provided during the Supplemental Extended Reporting Period, is excess over any other valid and collectible insurance that begins or continues in effect after the Supplemental Extended Reporting Period becomes effective, whether the other insurance applies on a primary, excess, contingent, or any other basis.

6. Identity Recovery Help Line

For assistance, if Identity Recovery applies, the "identity recovery insured" should call the **Identity Recovery Help Line** at **1-833-220-0327**.

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 Cyber Coverage. 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".

7. Legal Action Against Us

No one may bring a legal action against us under this insurance unless:

a. There has been full compliance with all of the terms of this insurance; and

b. The action is brought within two years after the date the "loss" or "identity theft" is first discovered by you, or the date on which you first receive notice of a "claim" or "regulatory proceeding".

8. Legal Advice

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

9. Other Insurance

a. If there is other insurance that applies to the same "loss", this Cyber Coverage shall apply only as excess insurance after all other applicable insurance has been exhausted.

b. If the same coverage applies under this Endorsement and any other coverage provided in this Policy, the coverage provided within this Endorsement supersedes any contrary terms, definitions, conditions and exclusions.

10. Pre-Notification Consultation

You agree to consult with us prior to the issuance of notification to "affected individuals". We assume no responsibility under 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 the Service Providers condition below. 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 fewer services in order to make those services available to more "affected individuals" without exceeding the available Data Compromise Response Expenses limit of insurance.

11. Service Providers

a. We will only pay under this Cyber Coverage 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 Cyber Coverage. 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.

12. 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 Cyber Coverage:

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 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 Cyber Coverage. Those firms work for you.

F. DEFINITIONS

1. "Affected Individual" means any person who is your current, former or prospective customer, client, patient, member, owner, student, director or employee and whose "personally identifying information" or "personally sensitive information" is lost, stolen, accidentally released or accidentally published by a "personal data compromise" covered under this Cyber Coverage. 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" must have a direct relationship with your interests as insured under this policy. The following are examples of individuals who would not meet this requirement:

(1) If you aggregate or sell information about individuals as part of your business, the individuals about whom you keep such information do not qualify as "affected individuals". However, specific individuals may qualify as "affected individuals" for another reason, such as being an employee of yours.

(2) If you store, process, transmit or transport records, the individuals whose "personally identifying information" or "personally sensitive information" you are storing, processing, transmitting or transporting for another entity do not qualify as "affected individuals". However, specific individuals may qualify as "affected individuals" for another reason, such as being an employee of yours.

(3) You may have operations, interests or properties that are not insured under this policy. Individuals who have a relationship with you through such other operations, interests or properties do not qualify as "affected individuals". However, specific individuals may qualify as "affected individuals" for another reason, such as being an employee of the operation insured under this policy.

c. 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 a director of you 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 director 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 at 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 you must submit or do submit with our consent;

   (4) Any other alternative dispute resolution proceeding in which such damages are claimed and to which you must submit or to which we agree you should submit to;

   arising from a "wrongful act" or a series of interrelated "wrongful acts" 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 director;

   (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. Includes a demand or proceeding arising from a "wrongful act" that is a "personal data compromise" only when:

   (1) The proceeding is brought by one or more "affected individuals";

   (2) The claimant alleges that one or more "affected individuals" suffered damages; and

(3) The "personal data compromise" giving rise to the proceeding was covered under Data Compromise Response Expenses section of this Cyber Coverage, and you submitted a "claim" to us and provided notifications and services to "affected individuals" in consultation with us pursuant to 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 is owned or leased by you and operated under your control.

9. "Coverage Term" means the increment of time:

a. Commencing on the earlier of the first inception date of this Cyber Coverage or the first inception date of any coverage substantially similar to that described in this Cyber Coverage and held immediately prior to this Cyber coverage; and

b. Ending upon the "termination of coverage".

10. "Coverage Territory" means:

a. With respect to Data Compromise Response Expenses, Computer Attack, Cyber Extortion and Identity Recovery, "coverage territory" means anywhere in the world.

b. With respect to Data Compromise Liability, Network Security Liability and 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" 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 you. 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 directors, 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:

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; or

c. A violation of a person's right of privacy, including false light and public disclosure of private facts.

18. "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.

19. "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":

a. 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".

b. 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".

c. Credit Reports

Costs for credit reports from established credit bureaus.

d. 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 an "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 Cyber Coverage or policy.

20. "Identity Recovery Insured" means the following:

a. When the entity insured under this Cyber Coverage is a sole proprietorship, the "identity recovery insured" is the individual person who is the sole proprietor of the insured identity.

b. When the entity insured under this Cyber Coverage is a partnership, the "identity recovery insureds" are the current partners.

c. When the entity insured under this Cyber Coverage 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.

An "identity recovery insured" must always be an individual person. If the entity insured under this Cyber Coverage is a legal entity, that legal entity is not an "identity recovery insured".

21. "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.

22. "Loss"

a. With respect to Data Compromise Response Expenses, "loss" means those expenses enumerated in Data Compromise Response Expenses, paragraph **b**.

b. With respect to Computer Attack, "loss" means those expenses enumerated in Computer Attack, paragraph **b**.

c. With respect to Cyber Extortion, "loss" means "cyber extortion expenses".

d. With respect to Data Compromise Liability, Network Security Liability and Electronic Media Liability, "loss" means "defense costs" and "settlement costs".

e. With respect to Identity Recovery, "loss" means those expenses enumerated in Identity Recovery, paragraph **b**.

23. "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.

24. "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; or

c. The unintended loss, release or disclosure of "third party corporate data".

25. "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".

26. "Personally Identifying Information"

a. "Personally identifying information" means information, including health information, that could be used to commit fraud or other illegal activity involving the 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.

27. "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".

28. "Policy Period" means the period commencing on the effective date shown in the Cyber Suite Supplemental Declarations. The "policy period" ends on the expiration date or the cancellation date of this Cyber Coverage, whichever comes first.

29. "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.

30. "Regulatory Proceeding" means an investigation, demand or proceeding alleging a violation of law or regulation arising from a "personal data compromise" 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.

31. "Settlement Costs"

a. "Settlement costs" means the following, when they arise from a "claim":

(1) Damages, 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 Data Compromise Response Expenses;

(2) Punitive and exemplary damages;

(3) The multiple portion of any multiplied damages;

(4) Taxes; or

(5) Matters which may be deemed uninsurable under the applicable law.

c. With respect to fines and penalties, the law of the jurisdiction most favorable to the insurability of those fines, or penalties will control for the purpose of resolving any dispute between us and you regarding whether the fines, or penalties specified in this definition above are insurable under this Cyber Coverage, provided that such jurisdiction:

(1) Is where those fines, or penalties were awarded or imposed;

(2) Is where any "wrongful act" took place for which such fines, or penalties 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.

32. "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 its pre-"computer attack" level of functionality:

(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";

(2) Labor costs of your employees or directors;

(3) Any costs in excess of the actual cash value of your "computer system"; or

(4) Costs to repair or replace hardware.

33. "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 date of the first inception of this coverage or any coverage substantially similar to that described in this Cyber Coverage.

34. "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 Cyber Coverage which is not available to the general public and is provided to you subject to a mutually executed written confidentiality agreement or which you are legally required to maintain in confidence.

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

35. "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.

36. "Wrongful Act"

a. With respect to Data Compromise Liability, "wrongful act" means a "personal data compromise".

b. With respect to Network Security Liability, "wrongful act" means a "network security incident".

c. With respect to Electronic Media Liability, "wrongful act" means an "electronic media incident".

All other terms, conditions and limitations of this Policy shall remain unchanged.