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 VI – DEFINITIONS.

SECTION I – COVERAGE

A. Response Expenses

Coverage is provided as described below when there has been a "personal data compromise" event which is first discovered by you during the policy period shown in the Declarations:

1. Legal And Forensic Information Technology Review

   We will pay your necessary and reasonable costs for the following outside professional services:
   a. Legal Services, meaning professional legal counsel review of the "personal data compromise" and how you should best respond to it; and
   b. Forensic Information Technology Services, meaning 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."

2. Notification To Affected Individuals

   We will pay your necessary and reasonable costs to provide notification of the "personal data compromise" to "affected individuals."

3. Services To Affected Individuals

   We will pay your necessary and reasonable costs to provide the following services to "affected individuals":
   a. Informational Materials, meaning a packet of loss prevention and customer support information;
   b. Help Line, meaning a toll-free telephone line for "affected individuals" with questions about the "personal data compromise" or wanting to request additional services as listed in c. and d. below;
   c. Credit Report and Monitoring, meaning 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; and
   d. Identity Restoration Case Management, meaning assisting an "affected individual", who is or appears to be a victim of an "identity theft" that may have reasonably arisen from the "personal data compromise", through the process of correcting credit and other records and, within what is necessary and reasonable, restoring control over their personal identity by providing the services of an identity restoration professional

B. Defense And Liability

We will pay for "data compromise defense costs" and "data compromise liability costs" you become legally obligated to pay as a result of a "data compromise suit" if you have provided notification and services to "affected individuals" in consultation with us pursuant to Response Expense Coverage and the suit is brought by one or more "affected individuals" and notice of the "data compromise suit" is received by you within two years of the date that the "affected individuals" were notified of the "personal data compromise"

SECTION II – EXCLUSIONS

We will not pay for costs arising from the following:

1. Your intentional or willful complicity in a "personal data compromise".
2. Any criminal, fraudulent or dishonest act, error or omission, or any intentional or knowing violation of the law by you.
3. Any "personal data compromise" event occurring prior to the first inception of this Coverage Form regardless of when the "personal data compromise" event was first discovered by you.
4. Except as specifically provided under Section – I.A.1.b. Forensic Information Technology Services, costs to research any deficiency including, but is not limited to, any deficiency in your systems, procedures or physical security that may have contributed to a “personal data compromise”.

5. Costs to correct any deficiency including, but not limited to, any deficiency in your systems, procedures or physical security that may have contributed to a “personal data compromise”.

6. Any fines or penalties including, but not limited to, fees or surcharges from affected financial institutions.

7. Any criminal investigations or proceedings.

8. Any threat, extortion or blackmail including, but not limited to, ransom payments and private security assistance.

9. Any virus or other malicious code that is or becomes named and recognized by the CERT Coordination Center, McAfee, Secunia, Symantec or other comparable third party monitors of malicious code activity.

10. Your reckless disregard for the security of “personally identifying information” in your care, custody or control.

11. That part of any “data compromise suit” seeking any non-monetary relief.

12. Seizure or destruction of property by order of governmental authority.

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

14. 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 a 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, or action taken by governmental authority in hindering or defending against any of these.

SECTION III – LIMITS OF INSURANCE

A. Response Expenses

The most we will pay under Response Expenses coverage is the Data Compromise Response Expenses Limit shown in the Declarations.

The Data Compromise Response Expenses Limit is a policy aggregate limit. This amount is the most we will pay for the total of all loss covered under Section I.A. arising out of all “personal data compromise” events which are first discovered by you during the policy period shown in the Declarations. This limit applies regardless of the number of “personal data compromise” events occurring during that period.

A “personal data compromise” event may be first discovered by you in one policy period but cause covered costs in one or more subsequent policy periods. If so, all covered costs arising from such “personal data compromise” event will be subject to the Data Compromise Response Expenses Limit applicable to the policy period when the “personal data compromise” was first discovered by you.

The most we will pay for loss under Legal And Forensic Information Technology Review coverage arising from any one “personal data compromise” event is $5,000. This limit is part of, and not in addition to, the Data Compromise Response Expenses Limit.

Coverage for Services To Affected Individuals 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.

B. Defense And Liability

The most we will pay under Defense And Liability coverage is the Data Compromise Defense And Liability Limit shown in the Declarations.

The Data Compromise Defense And Liability Limit is a policy aggregate limit. This amount is the most we will pay for all loss covered under Section I.B. arising out of all “personal data compromise” events which are first discovered by you during the policy period shown in the Declarations. This limit applies regardless of the number of “personal data compromise” events occurring during that period.

A “personal data compromise” may be first discovered by you in one policy period but cause covered costs in one or more subsequent policy periods. If so, all covered costs arising from such “personal data compromise” will be subject to the Data Compromise Defense and Liability Limit applicable to the policy period when the “personal data compromise” was first discovered by you.

SECTION IV – DEDUCTIBLE

A. Response Expenses

Response Expenses coverage is subject to a deductible of $2,500. You shall be responsible for such deductible amount as respects each “personal data compromise” event.

B. Defense And Liability

Defense And Liability coverage is subject to a deductible of $2,500. You shall be responsible for such deductible amount as respects each “data compromise suit”.

©2006, 2009 Hartford Steam Boiler Insurance Company

Includes copyrighted material of ISO Properties, Inc. with its permission.
SECTION V – CONDITIONS
The following conditions apply in addition to the Common Policy Conditions:

1. Abandonment
   There can be no abandonment of any property to us.

2. Concealment or Fraud
   This policy is void if you have intentionally concealed or misrepresented any material fact or circumstance relating to this insurance.

3. Coverage Territory
   The “personal data compromise” must involve “personally identifying information” that was within your care, custody or control within the United States of America and Puerto Rico.

4. Data Compromise Liability Defense
   a. We shall have the right, but not the duty, to assume the defense of any applicable “data compromise suit” against you. You shall give us such information and cooperation as we may reasonably require. In the event we do not assume your defense, we shall, nevertheless, have the right to effectively associate with you in the defense and settlement of any “data compromise suit” that appears reasonably likely to involve us, including, but not limited to, the right to effectively associate in the negotiation of a settlement.

   b. You shall not admit liability for or settle any “data compromise suit” or incur any defense costs without our prior written consent. However, if you are able to dispose of all "data compromise suits" which are subject to one deductible amount for an amount not exceeding the deductible amount (inclusive of defense costs), then our consent shall not be required for such claims and suits.

   c. If you refuse to consent to any settlement recommended by us and acceptable to the claimant, we may then withdraw from your defense (if we have assumed your defense) by tendering control of the defense to you. From that point forward, you shall, at your own expense, negotiate or defend such “data compromise suit” 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.

   d. We shall not be obligated to pay any damages or defense costs, or to defend or continue to defend any “data compromise suit” if we have assumed your defense, after the Data Compromise Defense and Liability Limit has been exhausted.

5. Defense Counsel
   We will only pay for “data compromise defense costs” for services provided by legal counsel approved by us. You must obtain our prior approval for any firm, service or legal counsel whose expenses you want covered as “data compromise defense costs.” We will not unreasonably withhold such approval.

6. Due Diligence
   You agree to use due diligence to prevent and mitigate costs covered under this Coverage Form. This includes, but is not limited to, complying 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,” including shredding hard copy files and destroying physical media used to store electronic data.

7. Duties in the Event of a Data Compromise Suit
   a. If a “data compromise suit” is brought against you, you must:
      1) Immediately record the specifics of the “data compromise suit” 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 “data compromise suit” is first received by you;
      3) Immediately send us copies of any demands, notices, summonses or legal papers received in connection with the “data compromise suit”;
      4) Authorize us to obtain records and other information;
      5) Cooperate with us in the investigation, settlement or defense of the “data compromise suit”;
      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 to which this insurance may also apply; and
      7) Take no action, or fail to take any required action, that prejudices your rights or our rights with respect to such “data compromise suit”.

©2006, 2009 Hartford Steam Boiler Insurance Company
DC7001(2-12) Includes copyrighted material of ISO Properties, Inc. with its permission.
b. You may not, except at your own cost, voluntarily make a payment, assume any obligation, or incur any expense without our prior written consent.

c. If you become aware of a claim or complaint that may become a "data compromise suit," you shall promptly inform us of such claim or complaint.

8. Duties in the Event of a Personal Data Compromise

You must see that the following are done in the event of a "personal data compromise":

a. Notify the police if a law may have been broken.

b. Give us prompt notice of the "personal data compromise". You must report the "personal data compromise" to us within 60 days of the date you first discover it.

c. As soon as possible, give us a description of how, when and where the "personal data compromise" occurred.

d. Take all reasonable steps to protect "personally identifying information" remaining in your care, custody or control. If feasible, preserve evidence of the "personal data compromise".

e. Permit us to inspect the property and records proving the "personal data compromise".

f. If requested, permit us to question you under oath at such times as may be reasonably required about any matter relating to this insurance or your claim, including your books and records. In such event, your answers must be signed.

g. Send us a signed, sworn statement containing the information we request to investigate the claim. You must do this within 60 days after our request. We will supply you with the necessary forms.

h. Cooperate with us in the investigation or settlement of the claim.

9. 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 "personal data compromise" is first discovered by you.

10. Legal Advice

We are not your legal advisor and do not provide legal counsel to you. None of the services we provide under this coverage constitute legal advice to you. Our determination of what is or is not covered under this Coverage Form does not represent advice or counsel from us about what you should or should not do.

11. Pre-Notification Consultation

You agree to consult with us prior to the issuance of notification to "affected individuals". We assume no responsibility under this Data Compromise Coverage 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 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"; and

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.

12. Service Providers

a. We will only pay under this Data Compromise Response Expenses 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 Data Compromise Coverage. We will not unreasonably withhold such approval.

b. Prior to the Pre-Notification Consultation described in Condition 11. 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; and

2) 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" by us, our designees or any service firm paid for in whole or in part under this Data Compromise coverage:

a. The effectiveness of such services depends on your cooperation and assistance.
b. All services may not be available or applicable to all individuals. For example, "affected individuals" 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. You will have a direct relationship with the professional service firms paid for in whole or in part under this coverage. Those firms work for you.

SECTION VI – DEFINITIONS

1. “Affected Individual” means any person who is your current, former or prospective customer, client, member, owner, director or employee and whose "personally identifying information" is lost, stolen, accidentally released or accidentally published by a “personal data compromise” covered under this Coverage Form. 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” 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. However, the coverage and services provided under this Coverage Form are only applicable and available within the Coverage Territory.

2. “Data Compromise Defense Costs” means expenses resulting solely from the investigation, defense and appeal of any “data compromise suit” against you. Such expenses must be reasonable and necessary. They may be incurred by us or by you with our written consent. They do not include your salaries or your loss of earnings. They do include premiums for any appeal bond, attachment bond or similar bond, but without any obligation to apply for or furnish any such bond.

3. “Data Compromise Liability Costs”

a. “Data compromise liability costs” means the following, when they arise from a “data compromise suit”:

1) Damages, judgments or settlements to “affected individuals”;

2) Defense costs added to that part of any judgment paid by us, when such defense costs are awarded by law or court order; and

3) Pre-judgment interest and post-judgment interest on that part of any judgment paid by us.

b. “Data compromise liability costs” does not mean:

1) Damages, judgments or settlements to anyone who is not an “affected individual”;

2) Civil or criminal fines or penalties imposed by law;

3) Punitive or exemplary damages;

4) The multiplied portion of multiplied damages;

5) Taxes; or

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

4. “Data Compromise Suit”

a. “Data Compromise Suit” means a civil proceeding in which damages to one or more “affected individuals” arising from a “personal data compromise” are alleged. Such proceeding must be brought in the United States of America, Puerto Rico or Canada. “Data compromise suit” includes:

1) An arbitration proceeding in which such damages are claimed and to which you must submit or do submit with our consent;

2) Any other alternative dispute resolution proceeding in which such damages are claimed and to which you submit with our consent; or
3) A written demand for money, when such demand could reasonably result in a civil proceeding as described in this definition.

b. “Data compromise suit” does not mean any demand or action brought by or on behalf of someone who is:
   1) Your director or officer;
   2) Your owner or part-owner; or
   3) A holder of your securities;
in their capacity as such, whether directly, derivatively, or by class action. “Data compromise suit” 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”.

c. “Data compromise suit” does not mean any demand or action brought by or on behalf of an organization, business, institution, governmental entity or any other party that is not an “affected individual”.

5. “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.

“Identity theft” does not include the fraudulent use of a business name, d/b/a or any other method of identifying a business activity.

6. “Personal Data Compromise” means the loss, theft, accidental release or accidental publication of “personally identifying information” as respects one or more “affected individuals,” if such loss, theft, accidental release or accidental publication has or could reasonably result 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” must be in your direct care, custody or control.

b. “Personal data compromise” does not include the loss, theft, release or publication of information that is in the care, custody or control of a third party to whom you have directly or indirectly turned over such information for any reason. This includes, but is not limited to, storage, processing, transmission or transportation of such information.

c. “Personal data compromise” includes disposal or abandonment of “personally identifying information” without appropriate safeguards such as shredding or destruction, subject to the following provisions:
   1) Your failure to use appropriate safeguards must be accidental and not reckless or deliberate; and
   2) Such disposal or abandonment must take place during the time period for which this Coverage Form is effective.

d. “Personal data compromise” includes situations where there is a reasonable cause to suspect that such “personally identifying information” has been lost, stolen, accidentally released or accidentally published, even if there is no firm proof.

e. 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.”

7. “Personally Identifying Information” means information that could be used to commit fraud or other illegal activity involving the credit or identity of an “affected individual”. This includes, but is not limited to, Social Security numbers or account numbers correlated with names and addresses.

“Personally identifying information” does not mean or include information that is otherwise available to the public, such as names and addresses with no correlated Social Security numbers or account numbers.