THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

DATA COMPROMISE COVERAGE
RESPONSE EXPENSES AND DEFENSE AND LIABILITY

Coverage under this endorsement is subject to the following:

PART 1 – RESPONSE EXPENSES

Data Compromise		
Response Expenses Limit:	$50,000	
	Annual Aggregate	
Sublimits		
Named Malware (Part. 1)	$50,000	
Forensic IT Review:	$ 5,000	
Legal Review:	$ 5,000	
PR Services:	$ 5,000	
		Any one *Personal Data Compromise*
Response Expenses Deductible:	$1,000	
		Any one *Personal Data Compromise*

PART 2 – DEFENSE AND LIABILITY

Data Compromise		
Defense and Liability Limit:	$50,000	
	Annual Aggregate	
Sublimits		
Named Malware (Part. 2)	$50,000	
		Any one *Personal Data Compromise*
Defense and Liability Deductible:	$1,000	
		Each *Data Compromise Suit*

Throughout this Coverage Endorsement (hereinafter referred to as Data Compromise Coverage), the words *you* and *your* refer to the *named insured(s)* shown in the Declarations and any organization(s) qualifying as a *named insured* under this Data Compromise Coverage. The words *we*, *us* and *our* refer to the company providing this insurance.

Other words and phrases that appear in *italics* have special meaning. Refer to the Glossary section of this endorsement.

The terms and conditions of the Cancellation/Termination Clauses of the Common Conditions and any amendment to such terms incorporated by endorsement are hereby incorporated herein and shall apply to coverage as is afforded by this Data Compromise Coverage, unless specifically stated otherwise in an endorsement(s) attached hereto.

PART 1 – RESPONSE EXPENSES

DATA COMPROMISE COVERED CAUSE OF LOSS

Coverage under this Data Compromise Coverage endorsement applies only if all of the following conditions are met:

1. There has been a *personal data compromise*; and
2. Such *personal data compromise* is first discovered by *you* during the policy period for which this Data Compromise Coverage endorsement is applicable; and
3. Such *personal data compromise* is reported to *us* within 60 days after the date it is first discovered by *you*.

COVERAGE – PART 1

If the three conditions listed above in DATA COMPROMISE – COVERED CAUSE OF LOSS have been met, then *we* will provide coverage for the following expenses when they arise directly from the covered cause of loss and are necessary and reasonable. Coverages 4 and 5 apply only if there has been a notification of the *personal data compromise* to *affected individuals* as covered under coverage 3.

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 PCI 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*.

a. The following services apply to any *personal data compromise*.

1) Informational Materials

A packet of loss prevention and customer support information.

2) 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 b. 1) and 2).

b. The following additional services apply to *personal data compromise* events involving *personally identifying information*.

1) 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.

2) 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. PR Services

Professional public relations firm review of and response to the potential impact of the *personal data compromise* on *your* business relationships.

This includes 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 promotions:

a. Provided to any of *your* directors or *employees*; or;

b. Costing more than $25 per *affected individual*.

LIMITS – PART 1

The most *we* will pay under Response Expenses coverage is the Data Compromise Response Expenses Limit indicated for this endorsement.

The Data Compromise Response Expenses Limit is an annual

aggregate limit. This amount is the most *we* will pay for the total of all loss covered under Part 1 arising out of all *personal data compromise* events which are first discovered by *you* during the present annual policy period. This limit applies regardless of the number of *personal data compromise* events discovered by *you* 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 Response Expenses Limit applicable to the period when the *personal data compromise* was first discovered by *you*.

The most *we* will pay under Response Expenses coverage for loss arising from any *malware-related compromise* is the Named Malware (Sec. 1) sublimit indicated for this endorsement. For the purpose of the Named Malware (Sec. 1) sublimit, all *malware-related compromises* that are caused, enabled or abetted by the same virus or other malicious code are considered to be a single *personal data compromise*. This sublimit is part of, and not in addition to the Data Compromise Response Expenses Limit.

The most *we* will pay under Forensic IT Review, Legal Review and PR Services coverages for loss arising from any one *personal data compromise* is the applicable sublimit for each of those coverages indicated for this endorsement. These sublimits are part of, and not in addition to, the Data Compromise Response Expenses Limit. PR Services coverage is also subject to a limit per *affected individual* as described in 5. PR Services.

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.

DEDUCTIBLE – PART 1

Response Expenses coverage is subject to the Response Expenses Deductible indicated for this endorsement. *You* shall be responsible for such deductible amount as respects each *personal data compromise* covered under this endorsement.

PART 2 – DEFENSE AND LIABILITY

DEFENSE AND LIABILITY COVERED CAUSE OF LOSS

Coverage under this Data Compromise Coverage endorsement applies only if all three of the conditions in DATA COMPROMISE – COVERED CAUSE OF LOSS are met.

Only with regard to Part 2 – Defense and Liability coverage, the following conditions must also be met:

1. *You* have provided notifications and services to *affected individuals* in consultation with *us* pursuant to Response Expenses coverage; and
2. *You* receive notice of a *data compromise suit* brought by one or more *affected individuals* or by a governmental entity on behalf of one or more *affected individuals*; and
3. Notice of such *data compromise suit* is received by *you* within two years of the date that the *affected individual* are notified of the *personal data compromise*; and
4. Such *data compromise suit* 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*.

COVERAGE – PART 2

If all of the conditions listed above in DEFENSE AND LIABILITY – COVERED CAUSE OF LOSS have been met, then *we* will provide coverage for *data compromise defense costs* and *data compromise liability* directly arising from the covered cause of loss.

LIMITS – PART 2

The most *we* will pay under Defense and Liability coverage (other than post-judgment interest) is the Data Compromise Defense and Liability Limit indicated for this endorsement.

The Data Compromise Defense and Liability Limit is an annual aggregate limit. This amount is the most *we* will pay for all loss covered under Part 2 (other than post-judgment interest) arising out of all *personal data compromise* events which are first discovered by *you* during the present annual policy period. This limit applies regardless of the number of *personal data compromise* events discovered by *you* 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* (other than post-judgment interest) 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*.

The most *we* will pay under Defense and Liability coverage for loss arising from any *malware-related compromise* is the Named Malware (Sec. 2) sublimit indicated for this endorsement. For the purpose of the Named Malware (Sec. 2) sublimit, all *malware-related compromises* that are caused, enabled or abetted by the same virus or other malicious code are considered to be a single *personal data compromise*. This sublimit is part of, and not in addition to, the Defense and Liability Limit.

DEDUCTIBLE – PART 2

Defense and Liability coverage is subject to the Defense and Liability Deductible indicated for this endorsement. *You* shall be responsible for such deductible amount as respects each *data compromise suit* covered under this endorsement.

EXCLUSIONS, ADDITIONAL CONDITIONS AND DEFINITIONS APPLICABLE TO BOTH PART 1 AND PART 2

EXCLUSIONS

The following additional exclusions apply to this coverage:

We will not pay for costs arising from the following:

1. *Your* intentional or willful complicity in a *personal data compromise.*
2. Any criminal, *fra*udulent or dishonest act, error or omission, or any intentional or knowing violation of the law by *you*.
3. Any *personal data compromise* occurring prior to the first inception of this Data Compromise Coverage endorsement or any coverage substantially similar to that described in this endorsement.
4. Costs to research or correct any deficiency. This includes, but is not limited to, any deficiency in *your* systems, procedures or physical security that may have contributed to a *personal data compromise*.
5. Any fines or penalties. This includes, but is not limited to, fees or surcharges from affected financial institutions.
6. Any criminal investigations or proceedings.
7. Any extortion or blackmail. This includes, but is not limited to, ransom payments and private security assistance.
8. Any *personal data compromise* involving data that is being transmitted electronically, unless such data is encrypted to protect the security of the transmission.
9. *Your* reckless disregard for the security of *personally identifying information* or *personally sensitive information* in *your* care, custody or control.
10. That part of any *data compromise suit* seeking any non-monetary relief.

ADDITIONAL CONDITIONS

The following Additional Conditions apply to all coverages under this endorsement.

A. Data Compromise Liability Defense

1. *We* shall have the right and 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.
2. *You* shall not admit liability for or settle any *data compromise suit* or incur any defense costs without *our* prior written consent.
3. 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 *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.
4. *We* shall not be obligated to pay any damages or defense costs, or to defend or continue to defend any *data compromise suit*, after the Data Compromise Defense and Liability Limit has been exhausted.
5. *We* shall pay all interest on that amount of any judgment within the Data Compromise Defense and Liability Limit 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 Data Compromise Defense and Liability Limit or, in any case, before *we* pay or offer to pay the entire Data Compromise Defense and Liability Limit.

   These interest payments shall be in addition to and not part of the Data Compromise Defense and Liability Limit.

B. Duties in the Event of a *Data Compromise Suit*

1. If a *data compromise suit* is brought against *you*, *you*

must:

a. Immediately record the specifics of the *data compromise suit* and the date received; and

b. 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*. Failure to give notice within the prescribed time shall not invalidate any claim if it shall be shown not to have been reasonably possible to give such notice within the prescribed time frame, that notice was given as soon as reasonably possible and that the insurer was not prejudiced by the failure to give notice within the prescribed time frame;

c. Immediately send *us* copies of any demands, notices, summonses or legal papers received in connection with the *data compromise suit*;

d. Authorize *us* to obtain records and other information;

e. Cooperate with *us* in the investigation, settlement or defense of the *data compromise suit*;

f. 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

g. Not take any action, or fail to take any required action, that prejudices *your* rights or *our* rights with respect to such *data compromise suit*.

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

3. 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.

C. Due Diligence

You agree to use due diligence to prevent and mitigate costs covered under this endorsement. This includes, but is not limited to, complying with, and requiring *your* vendors to comply with, reasonable and industry-accepted protocols for:

1. Providing and maintaining appropriate physical security for *your premises*, computer systems and hard copy files;

2. Providing and maintaining appropriate computer and Internet security;

3. Maintaining and updating at appropriate intervals backups of computer data;

4. Protecting transactions, such as processing credit card, debit card and check payments; and

5. Appropriate disposal of files containing *personally identifying information* or *personally sensitive information*, including shredding hard copy files and destroying physical media used to store electronic data.

D. Legal Advice

We are not *your* legal advisor. *Our* determination of what is or is not covered under this Data Compromise Coverage endorsement does not represent advice or counsel from *us* about what *you* should or should not do.

E. 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 Additional Condition F. Service Providers. *You* must provide the following at *our* pre-notification consultation with *you*:

1. The exact list of *affected individuals* to be notified, including contact information.

2. Information about the personal data compromise that may appropriately be communicated with *affected individuals*.

3. 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 Response Expenses Limit.

F. Service Providers

1. *We* will only pay under this Data Compromise 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.

2. Prior to the Pre-Notification Consultation described in Additional Condition E. 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:

   a. Such alternate service provider must be approved by *us*;

   b. 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

   c. *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.

G. 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:

1. The effectiveness of such services depends on *your* cooperation and assistance.
2. 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.
3. *We* do not warrant or guarantee that the services will end or eliminate all problems associated with the covered events.
4. *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*.

GLOSSARY

The following terms are defined for the purpose of this coverage form.

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* or *personally sensitive information* is lost, stolen, accidentally released or accidentally published by a *personal data compromise* covered under this endorsement. 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. *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 will be incurred by *us*. 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*
   a. *Data compromise liability* 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 on that part of any judgment paid by *us*.
   b. *Data compromise liability* 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* or the violation of a governmental statute or regulation 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 an organization, business, institution, or any other party that is not an *affected individual* or governmental entity. *Data compromise suit* does not mean any demand or action brought 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. *Malware-Related Compromise* means a *personal data compromise* that is caused, enabled or abetted by a virus or other malicious code that, at the time of the *personal data compromise*, is named and recognized by the CERT® Coordination Center, McAfee®, Secunia, Symantec or other comparable third party monitors of malicious code activity.

7. *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, subject to the following provisions:

1) The 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 Data Compromise Coverage endorsement is effective.

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*.

8. *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*. This includes, but is not limited to, Social Security numbers or account numbers.

Personally identifying information does not mean or include information that is otherwise available to the public, such as names and addresses.

9. *Personally Sensitive Information* means private information specific to an individual the release of which requires notification of *affected individuals* under any applicable law.

Personally sensitive information does not mean or include *personally identifying information*.

All other provisions of this policy apply.