

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

**NETWORK SECURITY ENDORSEMENT – INTEGRATED TECH
CLAIMS MADE
CLAIM EXPENSES INCLUDED WITHIN THE LIMITS OF INSURANCE**

This endorsement modifies insurance provided under the following:

TECHNOLOGY ERRORS AND OMISSIONS COVERAGE FORM – INTEGRATED TECH

SCHEDULE

Check Box	Supplemental Expense Coverage
<input type="checkbox"/>	Privacy Event Expense Your Security Breach Notification and Remediation Expenses Your Payment Card Expenses Your Crisis Management Service Expenses
<input type="checkbox"/>	Network Extortion Expense

In consideration of the payment of the premium and in reliance upon all statements and information furnished to **us** including all statements made in the application, its attachments and the material incorporated therein, which are incorporated herein and deemed to be a part of this policy, **we** agree as follows:

I. SECTION I – COVERAGE, A. Insuring Agreements, is amended to include the following:

A. Network Security Privacy Injury

We shall pay on **your** behalf all sums, not exceeding the limits of insurance and in excess of the applicable deductible shown in ITEM 4. in the Declarations, for which **you** shall become legally obligated to pay as **damages** resulting from any **claim** first made against **you** during the **policy period** or any subsequent extended reporting period, arising out of a **claim** for **network damage, privacy injury** and/or **privacy regulation proceeding** (including **privacy regulation fines**) by reason of a **wrongful incident**, committed after the retroactive date stated in ITEM 4. in the Declarations and prior to the end of the **policy period**, by an **insured** or by someone for whom an **insured** is legally responsible provided that:

1. The **wrongful incident** occurs in the **coverage territory**;
2. The **wrongful incident** occurs after the retroactive date shown in the Declarations and prior to the end of the **policy period**; and
3. **a.** The **claim** is first made against an **insured** during the **policy period** and reported to **us** in accordance with **SECTION V – GENERAL CONDITIONS, B. Notice & Claim Reporting Provisions**;
- b.** Prior to the inception date of this coverage form, no **executive officer** had knowledge of or should have known of any circumstances which might have resulted in a **claim**; and
- c.** The **wrongful incident**, or any **affiliated wrongful incident** has not been the subject

of any notice given under any previous coverage form.

Subject to any applicable limit of insurance, we will also pay **claim expenses** in connection with such covered **claim**.

B. Supplemental Expense Coverage

1. Privacy Event Expense

If the **privacy event expense** coverage has been purchased, as indicated by the check box in the endorsement **SCHEDULE** above, we will reimburse the **insured** for **privacy event expenses**, in excess of any applicable deductible and up to the applicable limit of insurance shown in ITEM 4. in the Declarations, that the **insured** has incurred to directly:

- a. Comply with:
 - (1) A **security breach notice law**; or
 - (2) Any statute or regulation referenced under the definition of **privacy injury** where the **insured** has been notified that a **privacy regulation proceeding** with respect to such law has been commenced; or
- b. Minimize harm to the **insured's** reputation from such **privacy event**, including but not limited to, setting up a call center and providing a credit monitoring service for those individuals impacted by a **privacy event**;

Provided, however, that all **privacy event expenses** must be:

- (1) Reported as soon as practicable, but in no event more than seven (7) days, after the **named entity's** notice of a **privacy event**;
- (2) Incurred within twelve (12) months of the date that the **insured** reports the event; and
- (3) Consented to in writing by **us**.

Each **security breach** in a series of **affiliated security breaches** will be deemed to occur on the date the first **security breach** in that series occurs.

2. Network Extortion Expense

If the **network extortion expense** coverage has been purchased, as indicated by the check box in the endorsement **SCHEDULE** above, **we** will reimburse the **insured** for **network extortion expense**, in excess of any applicable deductible and up to the applicable limit of insurance shown in ITEM 4. in the Declarations, that the **insured** incurred to directly respond to a **network extortion** demand that is made during the **policy period**; provided, however, that all **network extortion expense** must be:

- a. Reported to **us** as soon as practicable, but in no event more than seven (7) days of the **named entity's** receipt of a **network extortion** demand;
- b. Incurred within twelve (12) months of the date that the **insured** reports the **network extortion** demand to **us**; and
- c. Consented to in writing by **us**.

- II. For the purpose of this endorsement, **SECTION II – DEFINITIONS** is amended by deleting Definitions **D. Claim** and **EE. Wrongful incident** in their entirety and replacing them with the following:

D. Claim means:

1. A written demand for monetary damages or non-monetary relief (including demands for injunctive or declaratory relief) against an **insured** alleging a **wrongful incident**;
2. A formal civil administrative or regulatory proceeding or formal civil, administrative, including a **privacy regulation proceeding** or regulatory investigation, against an **insured**, alleging a **wrongful incident**, including any appeal therefrom. Such **claim** shall be deemed made on the earliest of the date of service upon or other receipt by any **insured** of a complaint, written notice of subpoena, or similar document of service in such proceeding, or arbitration; or
3. A written request received by the **insured** to toll or waive a statute of limitations in connection with a **claim** as defined in Paragraph 1. and 2. above.

Claim does not include any criminal proceeding; criminal or civil investigation; or any regulatory proceeding except if the regulatory proceeding is a **privacy regulation proceeding**.

EE. Wrongful incident means:

1. Solely with respect to any **network damage** coverage provided by this endorsement, any actual or alleged act, error, omission, neglect or breach of duty that results in any **security breach** of your **network**;
2. Solely with respect to any **privacy injury** coverage provided by this endorsement, any actual or alleged act, error, omission, neglect or breach of duty with respect to any information in durable and persistent form and in **your** care, custody or control; and
3. Solely with respect to any **privacy regulation** coverage provided by this endorsement, any matters that would qualify as a **wrongful incident** in Paragraphs 1. or 2. above to the extent such referenced coverages have been purchased.

III. **ADDITIONAL DEFINITIONS**

SECTION II – DEFINITIONS, is amended to include the following additional definitions:

A. Affiliated security breach means two or more **security breaches** that have as a common connection, tie, or link any fact, circumstance, situation, event, transaction, cause, or series of related facts, circumstances, situation, events, transactions, or causes.

B. Chargebacks:

1. Mean **payment card** charge reversals because of the fraudulent use of **payment cards** or **personally identifiable information**; and
2. Include transaction fees assessed to process such **payment card** charge reversals.

C. Denial of service attack means an attack executed over one or more **networks** or the internet, which attack is specifically designed and intended to disrupt the operation of a **network** and render a **network** inaccessible to authorized users.

D. Direct and continuous physical control means the laptop is:

1. Located within a facility occupied by the **insured**, where the **insured** physically limits access to the facility exclusively to **insureds** who are authorized by the **named entity** to access information on the laptop, and where the **insured** does not permit access by third parties unless they are escorted at all times by the **insured**;
 2. Within the **insured's** physical reach and unobstructed view while the **insured** is awake; or
 3. Within a locked container, vehicle, or premise which:
 - a. Can only be unlocked by an **insured**;
 - b. The **insured** has not entrusted the keys or combination (if secured by a combination lock) to a third party other than a third party custodian; or
 - c. Any such locked container is physically affixed to the structure of a building or premise in a manner that precludes its removal.
- E. Laptop computer breach** means the loss or theft of a laptop computer or a removable storage device that is:
1. In the **insured's direct and continuous physical control**; and
 2. Used by an **insured** for a business purpose; whether or not such laptop is lost or stolen from the **insured's** premises or from any third party's premises.
- F. Merchant service agreement** means a contract between **you** and an acquiring bank or other acquiring institution that establishes the terms and conditions for accepting and processing **payment card** transactions.
- G. Network** means a party's local or wide area network owned or operated by or on behalf of or for the benefit of that party; provided, however, **network** shall not include the internet, telephone company networks, or other public infrastructure network (collectively public infrastructure network) unless such public infrastructure network is operated and controlled exclusively by the **named entity**.
- H. Network damage** means:
1. The unscheduled and unplanned inability of an authorized user to gain access to the **network**;
 2. The unauthorized destruction or alteration of any third party's information residing on the **network**; or
 3. The suspension or interruption of the **network**.
- I. Network extortion** means a third party demand to the **named entity** for money or securities in exchange for:
1. The return of the **named entity's** confidential information or the confidential information of others in the **named entity's** care, custody or control;
 2. Not publicizing that the **named entity's network** will be or has been impaired, compromised or destroyed;
 3. Not impairing, altering or destroying the **named entity's network** or website; or

4. Not disclosing the **named entity's** confidential information or confidential information in its care, custody or control to unauthorized recipients;

Provided that the **named entity's executive officers** reasonably believe that the third party's demand is credible and that there is imminent and probable danger that the extortionist can execute on its demand.

- J. Network extortion expense** means all reasonable and necessary expenses incurred by the **named entity** in order to directly respond to a **network extortion**, including the payment of money or securities demanded by an extortionist; provided, however, that the payment of money or securities demanded by an extortionist must be made in conjunction with, and at the direct direction of, any law enforcement agency conducting an investigation of the **network extortion**.
- K. Nonpublic corporate information** means proprietary trade secret information owned by a third party that is in the care, custody or control of the **named entity** by operation of law or pursuant to a contractual obligation that requires the **named entity** to maintain the confidentiality of such proprietary trade secret information.
- L. Payment card** means a credit card, debit card or charge card issued by a financial institution.
- M. Payment card contract penalties** mean fines or penalties incurred by **you** after a **security breach** because of non-compliance with the **payment card security standards**.

Payment card contract penalties do not include:

1. Fines or penalties assessed because of not promptly reporting a **security breach**;
2. Fines or penalties assessed because of failure to properly validate system security according to the **payment card security standards**; and
3. Any interchange fees or changes in interchange fee schedules.

- N. Payment card security standards** mean:

1. The most current edition of security standards contained in:
 - a. The Payment Card Industry Data Security Standards program (PCI DSS);
 - b. Visa's Cardholder Information Security Program (CISP);
 - c. MasterCard's Site Data Protection program (SDP);
 - d. American Express's Data Security Operating Policy; or
 - e. Discover's Information Security and Compliance program (DISC); or
2. Other security standards similar to those in Paragraphs **1.a.** through **1.e.** above that **you** have agreed to in a **merchant service agreement** with a financial institution;

That apply to **you**.

- O. Payment card industry attestation of compliance** means the declaration of compliance status with the **payment card industry security standards** program found in the **payment card industry self-assessment questionnaire** that applies to **you**.

- P. Payment card industry forensic investigation** means a professional review of **your computer systems** by a **qualified forensic investigator** to determine **your** compliance with the **payment card security standards**.
- Q. Payment card industry self-assessment questionnaire** means the questionnaire developed by the Payment Card Industry Security Standards Council that assists **you** in self-evaluation of **your** compliance with the **payment card security standards**.
- R. Privacy event** means an act, error or omission by the **named entity**; by an **insured** within the scope of such individual's duties on behalf of the **named entity**; or by someone for whom the **insured** is legally responsible which, in the reasonable opinion of an **executive officer**, caused, or is reasonably likely to cause, the unauthorized disclosure of **personally identifiable information** or **nonpublic corporate information**.
- S. Privacy event expenses** means all reasonable and necessary fees, costs and expenses incurred by the **named entity** to directly respond to a **privacy event**. **Privacy event expenses** include, but are not limited to, the following:
1. **Your security breach notification and remediation expenses;**
 2. **Your payment card expenses;** and
 3. **Your crisis management service expenses.**
- T. Privacy injury** means:
1. Any unauthorized disclosure of, inability to access, inaccuracy in, or the **insured's** failure to prevent unauthorized access to **personally identifiable information**;
 2. The **insured's** failure to implement and maintain procedures designed to protect **personally identifiable information** from unauthorized use or disclosure, in violation of:
 - a. The **named entity's privacy policy**; or
 - b. Any federal, state, foreign or other law, statute or regulation governing the confidentiality, integrity, or accessibility of non-public personal information, including but not limited to the Health Insurance Portability and Accountability Act of 1996, Gramm-Leach-Bliley Act, Children's Online Privacy Protection Act, the EU Data Protection Act, or the Fair and Accurate Credit Transactions Act; and
 3. Any unauthorized disclosure of, inability to access, inaccuracy in, or an **insured's** failure to prevent unauthorized access to **nonpublic corporate information**.
- U. Privacy policy** means the **named entity's** policies in written or electronic form that:
1. Govern the collection, dissemination, confidentiality, integrity, accuracy or availability of **personally identifiable information**; and
 2. The **named entity** provides to those customers, employees or others who provide it with **personally identifiable information**.
- V. Privacy regulation fines** mean civil fines, sanctions or penalties imposed under any **privacy regulation proceeding** for a violation of any **security breach notice law** or any law, statute or regulation referenced under the definition of **privacy injury**.

- W. Privacy regulation proceeding** means a civil, administrative or regulatory proceeding against an **insured** by a federal, state or foreign governmental authority alleging a violation of any **security breach notice law** or any law, statute or regulation referenced under the definition of **privacy injury**.
- X. Qualified forensic investigator** means an organization approved by the applicable **payment card** issuing bank to conduct forensic investigations after a **security breach**.
- Y. Qualified security assessor** means a person or organization certified by the Payment Card Industry Security Standards Council to assess compliance with **payment card security standards**.
- Z. Security breach** means the failure of the **named entity's network** hardware, software, or firmware, the function or purpose of which is to:
1. Identify and authenticate parties prior to accessing the **named entity's network**;
 2. Control access to the **named entity's network** or monitor and audit such access;
 3. Protect against **malicious code**;
 4. Defend against **denial of service attacks** or co-option of the **named entity's network** to perpetrate a **denial of service attack** against others; or
 5. Ensure confidentiality, integrity and authenticity of information on the **named entity's network**.
- AA. Security breach notice law** means any statute or regulation that requires an entity storing **personally identifiable information** on its **network** to provide notice to specified individuals of any actual or potential **security breach** with respect to such **personally identifiable information**.
- BB. Software and hardware upgrade and scanning services expenses** mean:
1. Fees, costs or expenses for a **payment card industry forensic investigation** arising out of a written notification by a **payment card** issuing bank, merchant bank, acquiring bank or other acquiring institution that **you** are a likely common point of purchase source of a **security breach** or otherwise involved in a **security breach** to determine if **you** are in compliance with the **payment card security standards**;
 2. Costs or expenses to purchase and install anti-virus software, point-of-sale systems software, firewall protection software, or firewall protection hardware that satisfies the requirements of the **payment card security standards**, if, after a **security breach**, it is determined through a **payment card industry forensic investigation** that **you** are out of compliance with the **payment card security standards**; or
 3. Costs for the scanning services of a **qualified security assessor** to certify that **your** upgraded software and hardware systems meet the requirements of the **payment card security standards**, but only for the first such scanning services after **your** software or hardware systems, or both, are upgraded.
- CC. Your crisis management service expenses** mean the reasonable fees, costs or expenses incurred and paid by **you** in:
1. Retaining a public relations consultant or firm, or a crisis management consultant or firm; or

2. Planning or executing **your** public relations campaign;

To mitigate any actual or potential negative publicity generated from loss to which this insurance applies.

Your crisis management service expenses do not include fees, costs or expenses **you** incur to comply with any law or regulation.

DD. Your payment card expenses mean any of the following reasonable fees, costs or expenses incurred and paid by **you** which are directly attributed to a **security breach**:

1. **Software and hardware upgrade and scanning services expenses**;
2. **Payment card contract penalties**; or
3. **Chargebacks**.

Paragraphs **DD.2.** and **3.** above apply only if **you** have agreed to pay such **payment card contract penalties** or **chargebacks** in a **merchant service agreement you** entered into before such **security breach** occurred.

Your payment card expenses do not include:

- a. Remuneration paid to **your** regular employees for work beyond their normal scheduled hours;
- b. Fees, costs, or expenses of outside consultants retained by **you**, unless **we** agree to reimburse **you** for such fees, costs, or expenses;
- c. Amounts that **you** voluntarily agree to pay to any person whose **personally identifiable information** was accessed or acquired without his or her authorization;
- d. Fees, costs, or expenses in:
 - (1) Retaining a public relations consultant or firm, or a crisis management consultant or firm; or
 - (2) Planning or executing **your** public relations campaign;

To mitigate any actual or potential negative publicity generated from the **security breach**; or
- e. **Your security breach notification and remediation expenses**.

EE. Your security breach notification and remediation expenses mean any of the following reasonable fees, costs or expenses incurred and paid by **you** which can be directly attributed to a **security breach**:

1. Forensic fees, costs or expenses to determine the cause of the **security breach** and the persons whose **personally identifiable information** was accessed or acquired without their authorization;
2. Fees, costs or expenses to develop documents or materials to notify the persons whose **personally identifiable information** was accessed or acquired without their authorization;
3. Costs of mailings or other communications required to notify the persons whose **personally**

identifiable information was accessed or acquired without their authorization;

4. Costs of providing 365 days of credit monitoring services to persons whose **personally identifiable information** was accessed or acquired without their authorization, starting with the date that **you** first notify such persons of the **security breach**;
5. Costs of establishing and maintaining a call center to be used by persons whose **personally identifiable information** was accessed or acquired without their authorization; or
6. Any other fees, costs, or expenses necessary to comply with any **security breach notice law** that applies to **you**.

Your security breach notification and remediation expenses do not include:

- a. Remuneration paid to **your** regular employees for work beyond their normal scheduled hours;
- b. Fees, costs, or expenses of outside consultants retained by **you**, unless **we** agree to reimburse you for such fees, costs, or expenses;
- c. Fines or penalties imposed by law or that any **insured** has agreed to pay for any reason;
- d. Amounts that **you** voluntarily agree to pay to any person whose **personally identifiable information** was accessed or acquired without his or her authorization; or
- e. **Your crisis management service expenses.**

FF. Your work:

1. Means:
 - a. Work or operations performed by **you** or on **your** behalf; and
 - b. Materials, parts or equipment furnished in connection with such work or operations.
2. Includes:
 - a. Warranties or representations made at any time with respect to the fitness, quality, durability, performance or use of **your work**; and
 - b. The providing of or failure to provide warnings or instructions.

IV. For the purpose of this endorsement, **SECTION III – EXCLUSIONS** is amended as follows:

- A. Exclusion **B. Bodily Injury / Property Damage** is deleted in its entirety and replaced with the following:

Bodily Injury / Property Damage

For **bodily injury** including death, sickness, disease, emotional distress, or mental anguish of any person, or **property damage**. However, this exclusion shall not apply to the wrongful infliction of emotional distress or mental anguish arising out of **privacy injury**.

- B. Exclusion I. Unsolicited Communication** is deleted in its entirety and replaced with the following:

Unsolicited Communication / Spyware

Arising out of, resulting from, based upon or in consequence of:

1. Any actual or alleged violation of any federal or state anti-spam statute or regulation, including the CAN- SPAM Act of 2003;
2. Any actual or alleged violation of any federal or state statute or regulation prohibiting the dissemination of unsolicited electronic communications to multiple third parties, including any violation of the Telephone Consumer Protection Act of 2001; or
3. The distribution of unsolicited content including using pop-ups or other ad-ware without written permission of the recipient of such content.

However, this exclusion shall not apply to the extent such violation or such unsolicited distribution arises out of a **security breach**.

- C. Exclusion O. Insured vs. Insured** is amended by adding the following to the end of that exclusion:

Provided, however, that this exclusion shall not apply to:

1. Any **claim** that is in the form of a cross claim, third-party claim or otherwise for contribution or indemnity which is part of and results directly from a **claim** which is not otherwise excluded under this policy;
2. Any **claim** brought or maintained by or on behalf of a bankruptcy or insolvency trustee, examiner, liquidator, receiver or rehabilitator for **you** or any assignee of such trustee, examiner, liquidator, receiver or rehabilitator; or
3. Any **claim** brought by an employee for **privacy injury** or **network damage**.

V. ADDITIONAL EXCLUSIONS

SECTION III – EXCLUSIONS is amended to include the following additional exclusions:

This policy also does not apply to any **claim** or **claim expenses**:

A. Governmental Actions

Arising out of, resulting from, based upon or in consequence of any action or order by any domestic or foreign law enforcement, administrative, regulatory or judicial body or other governmental authority, to ban, limit or restrict access to, or provide access to, or intercept, confiscate, monitor or analyze, the **network** or any data, software or other information stored or processed on, or transmitted to or from, the **network**, whether authorized by the **insured** or not, including without limitation, interception, monitoring, or analysis by the NSA, CIA or FBI, or under the Foreign Intelligence Surveillance Act, the USA Patriot Act or any other domestic or foreign law, regulation or order.

B. Injunctive Relief

For the cost of any non-monetary relief, including without limitation, any costs associated with compliance with any injunctive relief of any kind or nature imposed by any judgment or

settlement. However, we shall provide a defense for any claim seeking injunctive relief. Such defense will not waive any of our rights under this policy.

C. Laptop Compromise

Arising out of, resulting from, based upon or in consequence of any **laptop computer breach** where the laptop was not under the **insured** or a third-party custodian's **direct and continuous physical control**, unless:

1. The information contained on the laptop was encrypted using a Federal Information Processing Standard (FIPS) 140-2 compliant whole disk encryption solution, and:
 2.
 - a. The encryption keys were generated and distributed in a manner that precludes access to such keys by unauthorized personnel;
 - b. The encryption includes a key recovery mechanism that ensures that encrypted information can only be decrypted and accessed by authorized personnel; and
 - c. The encryption key recovery mechanism requires approval by the **named entity's** senior management to authorize recovery of keys by anyone other than the key owner.

D. Payment Card Industry Attestation of Compliance

Arising out of **your payment card expenses** if:

1. **You** have not attested compliance with the **payment card security standards** by completing and signing a **payment card industry attestation of compliance** within the twelve (12) months immediately preceding the **security breach**; or
2. **You** fraudulently or intentionally misrepresent that **you** are in compliance with the **payment card security standards** in completing the **payment card industry attestation of compliance**.

E. Software

Arising out of, resulting from, based upon or in consequence of the inability to use or lack of performance of software programs:

1. Due to expiration, cancellation, withdrawal or failure to maintain or support said software programs;
2. That have not yet been released from their development stage, passed all test runs or proven successful in applicable daily operations; or
3. That result from the **insured's** modification of software programs in violation of any software license agreement, including but not limited to, violation of license provisions regarding modifications that invalidate a warranty; provided, however, this exclusion shall not apply to **your work** or **your product**.

F. Video Game Property

Arising out of, resulting from, based upon or in consequence of any theft or unlawful exchange of computer or video game currency, points, earnings, awards or other such intangible property.

VI. LIMITS OF INSURANCE

For the purpose of this endorsement, **SECTION IV – LIMITS OF INSURANCE** is deleted in its entirety and replaced with the following:

- A. The most we will pay for the sum of all **damages** and **claim expenses** for any one **privacy regulation proceedings claim** to which this insurance applies, is the Network Security Each Claim Limit of Insurance shown in ITEM 4. in the Declarations, if any. The applicable deductible shown in ITEM 4. in the Declarations shall apply to each and every **claim**, including **claim expenses**, and such deductible shall be borne by **you**. The deductible shall be uninsured and be at **your** own risk.
- B. The most we will pay for all **privacy event expenses** and **network extortion expenses** to which this insurance applies, is the applicable Each Claim Limit of Insurance shown in ITEM 4. in the Declarations, if any. The applicable deductible shown in ITEM 4. in the Declarations shall apply to each and every **claim** and such deductible shall be borne by **you**. The deductible shall be uninsured and be at **your** own risk.
- C. **Our** maximum aggregate liability for all **damages** arising out of all **claims** made and reported during the **policy period** shall be the Technology Errors and Omissions Policy Aggregate Limit of Insurance stated in ITEM 4. in the Declarations. The limit of insurance during any extended reporting period added to this policy shall be the remaining portion, if any, of the aggregate limit of insurance provided by this policy as stated in ITEM 4. in the Declarations.

Any Each Claim Limit of Insurance shown in ITEM 4. in the Declarations shall reduce, and shall in no way increase, the Technology Errors and Omissions Policy Aggregate Limit of Insurance as stated in ITEM 4. in the Declarations. Therefore any Each Claim Limit of Insurance is included within and not in addition to the Technology Errors and Omissions Policy Aggregate Limit of Insurance.

- D. **Claims** based on or arising out of the **wrongful incident** and any **affiliated wrongful incident** shall be considered a single **claim** and shall be considered first made during the **policy period** or the extended reporting period (if applicable), of the policy in which the earliest **claim** arising out of such act(s) or circumstance(s) was first made and all **damages** shall be subject to the same per **claim** limit of insurance.
- E. Payment by **us** of **claim expenses** incurred with any **claim**, shall serve to reduce the limit of insurance stated in ITEM 4. in the Declarations. Therefore, **claim expenses** are included within and not in addition to any applicable Each Claim Limit of Insurance or the Technology Errors and Omissions Policy Aggregate Limit of Insurance.

VII. ADDITIONAL CONDITION

For the purposes of this endorsement, **SECTION V – GENERAL CONDITIONS** is amended to include the following additional condition:

DUTIES IN THE EVENT OF A PRIVACY EVENT

You must see to it that **we** are notified in writing as soon as practicable, but in no event more than seven (7) days, after the **named entity's** notice of a **privacy event** which may result in **your security breach notification and remediation expense** or **your payment card expenses**.

1. Pursuant to **SECTION V – GENERAL CONDITIONS, C. Notice and Claim Reporting Provisions**, **you** shall give written notice containing:

- a. How, when and where the **security breach** occurred; and
- b. The nature and extent of fees, costs or expense incurred and paid by **you** which can be directly attributed to a **security breach**.

A **security breach** will be deemed to have been first reported to **us** on the date that **we** first receive a written notice of such **security breach** from any **insured** or any authorized government entity.

2. You must:

- a. Authorize **us** to obtain records and other information;
- b. Cooperate with **us** in the investigation of the **security breach**; and
- c. 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.

All other terms and conditions of the policy remain unchanged.

SPECIMEN