THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

CRISIS MANAGEMENT AND COMPUTER SYSTEM EXTORTION COVERAGE ENDORSEMENT

This endorsement modifies insurance provided under the following:

MISCELLANEOUS PROFESSIONAL LIABILITY INSURANCE POLICY

ENDORSEMENT PERIOD: «PolicyEffectiveDate» «to» «PolicyExpirationDate»
ENDORSEMENT RETROACTIVE DATE: «INSERT HERE»

Solely with respect to coverage afforded by this endorsement, in consideration of payment of premium and in reliance on the statements made and information furnished to the Insurer, including statements made in the **Application**, which is deemed attached to and a part of this policy, and subject to all other terms of this policy, the Insurer and the **Insured** agree to the following:

SCHEDULE

INSURING AGREEMENTS	***SUB-LIMIT OF LIABILITY***	***DEDUCTIBLE***
Crisis Management Coverage	$«CrisisManagementSub-Limit»	$«CrisisManagementDeductible»
Computer System Extortion Coverage	$«ExtortionSub-Limit»	$«ExtortionDeductible»

SECTION I., **INSURING AGREEMENTS**, of the policy is amended to add the following:

Crisis Management Coverage

The Insurer will reimburse **Crisis Management Expense**, in excess of the Deductible and within the applicable Sub-limit of Liability, paid by the **Insured** because of a **Wrongful Act** first occurring between the **Endorsement Retroactive Date** and the end of the **Policy Period** that results in an **Enterprise Security Event** first occurring during the **Policy Period**.

To be reimbursed, the **Insured** must notify the Insurer immediately after it has knowledge of the **Enterprise Security Event** and otherwise comply with all notice requirements and terms and conditions of this policy. Services to which Crisis Management Coverage applies must be delivered or performed as soon as practicable after the **Insured** notifies the Insurer of the **Enterprise Security Event**, but in no event later than one year after the **Enterprise Security Event** occurs.

Computer System Extortion Coverage

The Insurer will reimburse the **Insured** for **Extortion Expense** and/or **Extortion Loss**, in excess of the Deductible and within the applicable Sub-limit of Liability, paid by the **Insured** in order to prevent a **System Failure** or the unauthorized dissemination of **Protected Data** from the **Insured's Computer System**, because of a **Wrongful Act** first occurring between the **Endorsement Retroactive Date** and the end of the **Policy Period** that results in an **Extortion Threat** first made during the **Policy Period**. To be covered for **Extortion Expense** and/or **Extortion Loss**, the **Insured** must notify the Insurer of such **Extortion Threat** during the **Policy Period** immediately after the **Insured** has knowledge of the **Extortion Threat**.

SECTION II., **DEFINITIONS, "Wrongful Act"** of the policy is deleted in its entirety and replaced by the following:

"**Wrongful Act**" means conduct or alleged act, breach of duty, error or omission by an **Insured**, or any person or organization for whom an **Insured** is legally liable in its capacity as such. All **Interrelated Wrongful Acts** regardless of the number of repetitions, alterations, actions, or forms of communication shall be treated as one **Wrongful Act**.

SECTION II., **DEFINITIONS** of the policy is amended to add the following:

Claim Expense is amended to add the following to the end thereof:

Extortion Expense;
Extortion Loss; and
Crisis Management Expense.

Corporate Information means, with respect to a third party organization, any information held by the **Insured**: 1) that is subject to any form of confidentiality agreement or confidentiality provision in a contract or agreement between the organization and any **Insured Company**; or 2) which the **Insured Company** is legally required to maintain in confidence.

Provided, however, **Corporate Information** shall not mean and does not include **Protected Personal Information** or any publicly available information that is lawfully in the public domain or information available to the general public from government records.

Credit Monitoring Services means provision of single-bureau credit monitoring, at the election of the **Insured**, at the time notification is provided, to qualified persons if any one of the following types of information has been actually or allegedly improperly accessed, lost or stolen, in addition to such person's name or equivalent information used for the purpose of identifying such person:

1. Social Security Number or equivalent;

2. Driver's license or state identification number or equivalent; or

3. Account, credit card, or debit card number, alone or in combination with any information that permits access to an individual's financial information.

"Qualified persons" as used in this definition mean those natural, living persons to whom notification is given under this policy and who elect to receive monitoring services. Coverage for **Credit Monitoring Services** will be limited to the one (1) year period following the qualified person's receipt of notification of the **Enterprise Security Event**.

"Notification" as used in this definition means preparing and sending individual notification by reasonable means to customers and clients of the **Insured** and to any other person or party whose **Protected Personal Information** may have been improperly accessed, lost or stolen, provided however, this provision shall only apply to the extent the **Insured** is required to comply with **Privacy Regulations**.

Crisis Management Expense means reasonable amounts paid by the **Insured** to a third party in connection with 1. - 3. below, in excess of the **Insured's** normal operating costs and with the prior written approval of the Insurer following an **Enterprise Security Event** for the purpose of mitigating **Claim Expense** or **Damages** resulting from an **Enterprise Security Event**:

1. Hiring a public relations firm, law firm or crisis management firm approved by the Insurer, for advertising or other communications services following an **Enterprise Security Event**;

2. Placing advertisements and other communications recommended by a firm approved by the Insurer in 1. above, to explain the nature of the **Enterprise Security Event** and any corrective actions taken;

3. Preparing and sending individual notification by reasonable means to customers and clients of the **Insured** and to any other person or party whose **Protected Personal Information** may have been improperly accessed, lost or stolen, provided however, this provision shall only apply to the extent the **Insured** is required to comply with **Privacy Regulations.**

4. Providing **Credit Monitoring Services**.

Provided, however, **Crisis Management Expense** does not mean identity restoration services, investigation services to determine the cause of an **Enterprise Security Event**, services to identify, enroll or catalog the individuals' names, addresses or information that may have been improperly, accessed, lost or stolen, nor to determine if notification is required, forensics, preservation of evidence, nor any similar expense. Provided, further, reimbursement of expense under section 1. and 2. of this definition shall be part of, limited to and shall not exceed 5% of the Crisis Management Sub-Limit of Liability. All such reimbursement shall be in excess of the applicable Deductible and subject to all other limitations of this policy. Furthermore, all such expense must be incurred as soon as practicable after the Insured has knowledge of the **Enterprise Security Event**; **Crisis Management Expense** must be incurred within one year of the date the **Enterprise Security Event** first occurs; and **Crisis Management Expense** does not include salary charges, overhead or expenses of regular employees of the Insured.

Endorsement Period means the period specified at the top of the first page of this endorsement.

Endorsement Retroactive Date means the retroactive date specified on the top of this endorsement. If no retroactive date is provided, then the effective date of this endorsement.

Enterprise Security Event means any of the following:

1. Accidental release, unauthorized disclosure, theft, or loss of **Protected Personal Information** by the **Insured** or **Service Contractor**; or

2. The failure to prevent any of the following:

    a. Unauthorized access to or unauthorized use of **Protected Data** on the **Insured's Computer System** that directly results in alteration, destruction, deletion, corruption or damage to **Protected Data**;

    b. Transmitting or receiving **Malicious Code** via the **Insured's Computer System**; or

    c. Unauthorized access to or unauthorized use of the **Insured's Computer System** that directly results in denial or disruption of access of authorized parties.

All **Enterprise Security Events** that involve the same or related subject, person, class of persons or have common facts or circumstances or involve common transactions, events or decisions, regardless of the number of repetitions, alterations, actions, or forms of communication will be treated as one **Enterprise Security Event**.

Extortion Expense means the **Insured's** reasonable expenses to retain a negotiator approved by the Insurer, where such expenses are in excess of the normal operating costs of the Insured's business and are directly in response to a covered **Extortion Threat**. **Extortion Expense** does not include salary charges or expenses of regular employees of the Insured.

Extortion Loss means any funds paid by or on behalf of an Insured to a party or parties that have made an **Extortion Threat** in order to prevent a **System Failure** or the unauthorized dissemination of **Protected Data** from the **Insured's Computer System**; except **Extortion Loss** shall not include any amounts involving or connected with royalties, fees, deposits, commissions or charges for content, goods or services.

Extortion Threat means any credible threat or series of related threats, demanding payment of funds to avoid a **System Failure** or to avoid the release, disclosure, or theft of **Protected Data** from the **Insured's Computer System**. Provided, however, **Extortion Threat** shall not mean and shall not include a threat based upon, arising out of, or in connection with royalties, fees, deposits, commissions or charges for content, goods or services. All **Extortion Threats** that involve the same or related subject, person, class of persons or have common facts or circumstances or involve common transactions, events or decisions, regardless of the number of repetitions, alterations, actions, or forms of communication will be treated under this endorsement as one **Extortion Threat**.

Insured's Computer System means computers and associated input and output devices, data storage devices, networking equipment, and back-up facilities operated by and either owned by or leased to the **Insured Company**; or operated for the benefit of the **Insured Company** by a third party service provider and used for the purpose of providing hosted application services to the **Insured Company**; or for processing, maintaining, or storing electronic data, pursuant to a written agreement with the **Insured Company**.

Interrelated Wrongful Acts means all **Wrongful Acts** that have as a common nexus any fact, circumstance, situation, event, transaction, cause or series of causally or logically connected facts, circumstances, situations, events, transactions, or causes.

Malicious Code means any computer virus, Trojan horse, worm, or other code, script, or software program that is intentionally designed and released or inserted to damage, harm or infect any or all parts of a computer network and/or **Protected Data** on such a network.

Privacy Regulation means any of the following statutes and regulations associated with the care, custody, control or use of personally identifiable financial, medical or other sensitive personal information:

1. Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191);

2. Health Information Technology for Economic and Clinical Health Act of 2009, and its related regulations;

3. Gramm-Leach-Bliley Act of 1999;

4 California Database Breach Act (SB1386);

5. Minnesota Plastic Card Security Act; or

6. Other similar state, federal and foreign identity theft and privacy protection legislation that requires commercial entities that collect, process or store **Protected Personal Information** to post privacy policies, adopt specific privacy controls, or notify natural persons and/or organizations in the event that **Protected Personal Information** has been comprised.

Protected Data means **Protected Personal Information** and **Corporate Information**.

Protected Personal Information means, with respect to natural persons, any private, non-public or public information of any kind maintained by the **Insured** or by a party for whom the **Insured** is legally responsible regardless of the nature or form of such information, including but not limited to the following, but only to the extent that such information allows an individual to be uniquely identified:

1. Social Security Number;

2. Medical service or healthcare data;

3. Driver's license or state identification number;

4. Equivalents of any of the information listed in 1. to 3. above;

5. Account, credit card, or debit card number alone or in combination with any information that permits access to an individual's financial information including but not limited to security or access code or password; and

6. Other public or non-public information to the extent protected under **Privacy Regulations**.

Service Contractor means any organization that processes, maintains, or stores **Protected Personal Information** on behalf of the **Insured Company**, pursuant to a written agreement with the **Insured Company**.

System Failure means any of the following:

1. Unauthorized access to or unauthorized use of **Protected Data** on the **Insured's Computer System** that directly results in alteration, destruction, deletion, corruption or damage to **Protected Data**;

2. Transmitting or receiving **Malicious Code** via the **Insured's Computer System**; or

3. Unauthorized access to or unauthorized use of the **Insured's Computer System** that directly results in denial or disruption of access of authorized parties to online services.

SECTION IV., **LIMITS OF LIABILITY AND DEDUCTIBLE, A.**2 is replaced with the following:

Total Limit of Liability

The Total Limit of Liability stated in Item 5.b. on the Declarations Page is the most the Insurer will pay for **Damages** and **Claim Expense** combined.

SECTION IV., **LIMITS OF LIABILITY AND DEDUCTIBLE, A.**3. Sub-limits, of the policy is amended to add the following provisions:

Crisis Management and **Computer System Extortion** Sub-limits

The most the Insurer will pay for the total of all **Crisis Management Expense** shall be the amount stated in the Schedule, and the most the Insurer will pay for the total of all **Extortion Expense** and **Extortion Loss** shall be the amount stated in the Schedule, no matter how many:

1. **Insureds** this policy covers;
2. **Claims** are made;
3. Entities or persons bring **Claims**;
4. **Wrongful Acts** occur;
5. **Enterprise Security Events** occur; or
6. **Extortion Threats** are made;

Provided, however, that the Insurer's obligation to reimburse amounts under sections 1. and 2. of the definition of **Crisis Management Expenses** shall be part of, limited to and shall not exceed 5% of the Crisis Management Sub-Limit of Liability. All such reimbursement shall be in excess of the applicable Deductible and subject to all other limitations of this policy.

If the amount entered in the Schedule of this endorsement for a Sub-limit is Not Applicable (N/A), blank or zero (0), this policy provides no coverage for that sub-limited activity or coverage.

These Sub-limits, and any other Sub-limit which may be stated in any endorsement to this policy, shall be part of, and not in addition to, the Total Limit of Liability stated in Item 5.b. of the Declarations. Payment for **Crisis Management Expense**, **Extortion Threat** and/or **Extortion Loss** to which a Sub-limit applies will reduce the Total Limit of Liability available under this policy.

SECTION IV., **LIMITS OF LIABILITY AND DEDUCTIBLE**, **B. Deductible**, is amended by the addition of the following provisions at the end thereof:

Crisis Management and **Computer System Extortion** Deductibles

The Crisis Management Deductible applies to all **Crisis Management Expense** incurred as a result of each actual or alleged **Enterprise Security Event** covered by **SECTION I.**, **INSURING AGREEMENTS**, **Crisis Management Coverage** of this endorsement, and the Insurer's obligation to reimburse such **Crisis Management Expense** applies only to the amount of **Crisis Management Expense** in excess of this Deductible.

The Computer System Extortion Deductible applies to all **Extortion Expense** and **Extortion Loss** incurred as a result of each actual or alleged **Extortion Threat** covered by **SECTION I.**, **INSURING AGREEMENTS**, **Computer System Extortion** of this endorsement, and the Insurer's obligation to reimburse such **Extortion Expense** and **Extortion Loss** applies only to the amount of **Extortion Expense** and **Extortion Loss** in excess of this Deductible.

The amounts of the **Insured's** Deductibles are stated in the Schedule of Coverage. The Deductibles do not deplete the applicable sub-limit of Liability. If the amount entered into the Schedule for any Deductible is blank then the Deductible shall be 5% of the applicable Sub-limit.

At the Insurer's option, if the Insurer has paid any amounts for **Crisis Management Expense, Extortion Expense** or **Extortion Loss** in excess of the applicable Sub-limit of Liability, including any amounts paid in excess of the Insurer's

obligation to reimburse amount pursuant to this endorsement, or if the Insurer has paid part or all of any Deductible, the **Insured** shall reimburse the Insurer for such amounts upon demand.

SECTION V., **TERRITORY, CLAIMS MADE AND EXTENDED REPORTING PERIOD PROVISIONS**, **A.** and **B.** of the policy are deleted in their entirety and replaced by the following:

A. Territory

Coverage under this endorsement applies to **Enterprise Security Events**, **Wrongful Acts** and **Extortion Threats** taking place anywhere. If any amounts covered by this policy are paid in a currency other than United States of America dollars, then the payment under this policy will be considered to have been made in United States dollars at the conversion rate published in *The Wall Street Journal* at the time of payment.

B. **Reporting Provisions For Coverage Provided By This Endorsement**

In order for coverage to apply, the **Insured** must notify the Insurer of the **Enterprise Security Event** or **Extortion Threat** for which it intends to seek coverage immediately after the **Insured** has knowledge of such event and in accordance with **Section VII. GENERAL CONDITIONS**, **C.**, but in no event later than thirty (30) days after the end of the **Policy Period**.

No Automatic or Optional Extended Reporting Period options are available for coverage provided by this endorsement.

Furthermore:

a. **Crisis Management Coverage**

In order for coverage to apply, an **Enterprise Security Event** must result from a **Wrongful Act** that first occurs after the **Retroactive Date** but before the end of the **Policy Period,** no matter how many repetitions, alterations, actions, or forms of communication are involved or subsequently result.

The **Enterprise Security Event** must also first occur during the **Policy Period**. All **Enterprise Security Events** arising from the same **Wrongful Act** or **Interrelated Wrongful Acts** will be considered one **Enterprise Security Event** under this policy. An **Enterprise Security Event** shall be deemed to occur when the first of such **Enterprise Security Events** occurs.

b. **Computer System Extortion Coverage**

In order for coverage to apply, an **Extortion Threat** must result from a **Wrongful Act** that first occurs between the **Retroactive Date** and the end of the **Policy Period**, no matter how many repetitions, alterations, actions, or forms of communication are involved or subsequently result.

The **Extortion Threat** must be first made during the **Policy Period**, no matter how many repetitions, alterations, actions, or forms of communication are involved or subsequently result. All **Extortion Threats** arising from the same **Wrongful Act** or **Interrelated Wrongful Acts** will be considered one **Extortion Threat**. An **Extortion Threat** shall be deemed to occur when the first of such related **Extortion Threats** occurs.

SECTION VII., **GENERAL CONDITIONS**, **C., E.** and **L.** of the policy is deleted in its entirety and replaced by the following:

C. Insured's Duties in the Event of a Enterprise Security Event, Wrongful Act or Extortion Threat

1. If there is an **Enterprise Security Event, Wrongful Act** or **Extortion Threat**, the **Insured** must do the following after the **Insured Company** has knowledge of the **Enterprise Security Event**, **Wrongful Act** or **Extortion Threat**:

   a. Notify the Insurer in writing immediately. This notice must contain details that identify the **Insured**, the claimant and also reasonably obtainable information concerning the time, place and other details of the **Enterprise Security Event**, **Wrongful Act** or **Extortion Threat**;

b. Immediately send the Insurer copies of all demands, notices, summonses or legal papers received in connection with the **Enterprise Security Event**, **Wrongful Act** or **Extortion Threat**;

c. Authorize the Insurer to obtain records and other information;

d. Cooperate with and assist the Insurer in investigation, settlement, defense, and mitigation; and

e. Assist the Insurer, upon the Insurer's request, in enforcing any rights of contribution or indemnity against another who may be liable to any **Insured**.

2. No **Insured** will, except at the **Insured's** own cost, voluntarily make a payment, admit liability, assume any obligation or incur any expense without the Insurer's prior written consent.

3. When this policy requires that an **Insured** provide notice, we will consider the **Insured** to have knowledge of only when the **Insured Company's** chairperson of the board of directors, president, chief executive officer, chief operating officer, chief financial officer, chief security officer, chief technology officer, chief privacy officer, chief information security officer, risk manager or in-house counsel has that knowledge.

4. The **Insured** will in all respects cooperate with, and provide information requested by, the Insurer with respect to any **Enterprise Security Event**, **Wrongful Act** or **Extortion Threat** for which insurance is afforded under this endorsement and, at the Insurer's request, assist in mitigating **Crisis Management Expense, Extortion Expense**, **Extortion Loss** and making settlements and in enforcing any right of contribution or indemnity against any person or organization who may be liable to the **Insured**. The **Insured** will attend hearings and trials and assist in securing and giving evidence and obtaining the attendance of witnesses.

5. The Insurer shall not be obligated to reimburse **Extortion Expense** and **Extortion Loss**:

   a. If the **Insured** does not obtain the Insurer's prior written consent for such payments;

   b. If the **Insured** makes any payments to person(s) the Insurer does not reasonably believe to be responsible for and capable of terminating or ending the **Extortion Threat**;

   c. If or to the extent such payments exceed an amount the Insurer reasonably believes is necessary to terminate or end such **Extortion Threat**; or

   d. If or to the extent the reimbursement of **Extortion Expense** and **Extortion Loss** exceeds the greater of:

      (1) The Computer System Extortion sub-limit of this endorsement; or

      (2) The amount the Insurer reasonably believes to be the total of all **Damages** and **Claim Expense** for which the Insurer would be liable had the funds not been paid.

6. The **Insured** shall use its best efforts at all times to ensure that knowledge regarding the existence of the Computer System Extortion Coverage afforded by this policy is kept confidential. The Insurer may cancel the Computer System Extortion Coverage under this policy upon ten (10) days written notice to the **First Named Insured** if the existence of the Computer System Extortion Coverage provided by this policy becomes public knowledge or is revealed to a person making an **Extortion Threat** through no fault of the Insurer.

E. Other Insurance

If other valid and collectible insurance applies to a **Claim, Wrongful Act, Enterprise Security Event** or **Extortion Threat** covered under this policy, this insurance is excess over such other insurance, except when the other insurance is specifically arranged by or on behalf of the **Insured Company** to apply in excess of this insurance, and no other insurance applies to the **Claim, Wrongful Act, Enterprise Security Event** or **Extortion Threat**.

L. Severability

With regard to the information provided on any insurance **Application** or with regard to knowledge of any **Enterprise Security Event, Extortion Threat**, **Wrongful Acts** or **Claims** as referenced in this policy, only facts pertaining to and knowledge possessed by any of the offices of the **Insured Company's** chairpersons of the board of directors,

presidents, chief executive officers, chief operating officers, chief financial officers, risk managers, in-house counsels or any persons whose signature appears on any **Application**, shall be imputed to the **Insured**.

The terms and conditions of this endorsement will not operate to increase the Limit of Liability.

Except as stated above, this endorsement does not change any other provisions of this policy.

Endorsement No.
This endorsement, effective at 12:01 a.m.
forms a part of Policy number
issued to

Authorized Representative