



NETWORK RISK AND PRIVACY CLAIM ENDORSEMENT

In consideration of the premium paid for this Policy, it is understood and agreed that the Policy is amended as follows:

1. Section **III. DEFINITIONS**, the definition of **Claim** is amended to include the following:

“**Claim**” also includes:

- a) **privacy claims**, and
- b) **client network damage claims**.

2. Solely with respect to the coverage provided by this endorsement, Section **III. DEFINITIONS** is amended to add the following terms:

“**Client network damage claim**” means a demand, including the service of suit or the institution of any alternative dispute resolution proceeding, received by the **Insured** for money or services alleging that a **security breach** or **electronic infection** caused **network damage** to a client’s **network** in the rendering of **legal services**.

“**Computer virus**” means unauthorized computer code that is designed and intended to transmit, infect and propagate itself over one or more **networks**, and cause:

1. a computer code or programs to perform in an unintended manner;
2. the deletion or corruption of electronic data or software; or
3. the disruption or suspension of a **network**.

“**Confidential Commercial Information**” means information that has been provided to the **Insured** by another, or created by the **Insured** for another where such information is subject to the terms of a confidentiality agreement or equivalent obligating the **Insured** to protect such information on behalf of another.

“**Denial of service attack**” means an attack executed over one or more **networks** or the **Internet** that is specifically designed and intended to disrupt the operation of a **network** and render a **network** inaccessible to authorized users.

“**Electronic infection**” means the transmission of a **computer virus** to a **network**, including without limitation, such transmission to or from the **Named Insured’s network**.

“**Electronic information damage**” means the destruction, deletion or alteration of any information residing on the **network** of any third party.

“**Internet**” means the worldwide public **network** of computers as it currently exists or may be manifested in the future, but **Internet** does not include the **Named Insured’s network**.

“**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**.

“**Network Damage**” means:

1. the unscheduled and unplanned inability of an authorized user to gain access to a **network**;
2. **electronic information damage**; or
3. the suspension or interruption of any **network**;

“**Non-public personal information**” means personal information not available to the general public from which an individual may be identified, including without limitation, an individual’s name, address, telephone number, social security number, account relationships, account numbers, account balances, and account histories.



“**Privacy claim**” means a demand, including the service of suit or the institution of any alternative dispute resolution proceeding, received by the **Insured** for money or services and alleging **privacy injury and identity theft** that occurred in the rendering of **legal services**.

“**Privacy injury and identity theft**” means:

- a. any unauthorized disclosure of, inability to access, or inaccuracy with respect to, **non-public personal information** in violation of:
 1. the **Named Insured’s privacy policy**; or
 2. 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, or the EU Data Protection Act.
- b. the **Insured’s** failure to prevent **unauthorized access** to **confidential commercial information**;

“**Privacy policy**” means the **Named Insured’s** policies in written or electronic form that:

1. govern the collection, dissemination, confidentiality, integrity, accuracy or availability of **non-public personal information**; and
2. the **Insured** provides to its clients, customers, employees or others who provide the **Insured** with **non-public personal information**.

“**Security breach**” means the failure of the **Named Insured’s network** hardware, software, firmware, the function or purpose of which is to:

1. identify and authenticate parties prior to accessing the **Named Insured’s network**;
2. control access to the **Named Insured’s network** and monitor and audit such access;
3. protect against **computer viruses**;
4. defend against **denial of service attacks** upon the **Insured** or unauthorized use of the **Insured’s network** to perpetrate a **denial of service attack**; or,
5. ensure confidentiality, integrity and authenticity of information on the **Insured’s network**.

Privacy breach notice law means any statute or regulation that requires an entity who is the custodian of **non-public personal information** to provide notice to individuals of any actual or potential privacy breach with respect to such **non-public personal information**. **Privacy breach notice laws** include Sections 1798.29 and 1798.82- 1798.84 of the California Civil Code (formerly S.B. 1386) and other similar laws in any jurisdiction.

Unauthorized access means any accessing of information in the **Insured’s** care, custody or control by unauthorized persons or by authorized persons accessing or using such information in an unauthorized manner.

Unauthorized access also includes:

1. theft from the **Insured** of any information storage device used by the **Insured** to:
 - A. store and retrieve information on the **Insured’s network**; or
 - B. transport information between the **Insured** and authorized recipients;
2. any unauthorized use by the **Insured** of information in the **Insured’s** clients’ care, custody or control if accessed by the **Insured** in the course of rendering **legal services**.

3. The following new Section is added to the Policy:

- **Supplementary Payments: Regulatory Inquiry**

If, during the **policy period**, a state licensing board, self regulatory body, public oversight board or a governmental agency with the authority to regulate the **Insured’s legal services** or any entity acting on behalf of such entities initiates an investigation of **the Insured** arising from an actual or alleged violation of a **privacy breach notice law** or any law referenced under the definition of **privacy injury and identity theft** that occurred in the rendering of **legal services** and which the **Insured** reports to the **Company** in accordance with Section V.A. of this Policy, the **Company** agrees to pay attorney fees, attorney costs and court costs (excluding such attorney fees and costs incurred as a result of services performed by the **Insured**) incurred in responding to the investigation. The maximum amount the **Company** will pay for



such attorney fees and costs is \$20,000 regardless of the number of investigations or the number of **Insureds** who are subject to such investigations.

This endorsement shall not be construed as to increase the Limits of Liability of this Policy.

All other terms and conditions of the Policy remain unchanged.

This endorsement, which forms a part of and is for attachment to the Policy issued by the designated Insurers, takes effect on the effective date of said Policy at the hour stated in said Policy and expires concurrently with said Policy unless another effective date is shown below.

By Authorized Representative _____
(No signature is required if issued with the Policy or if it is effective on the Policy Effective Date)

SAMPLE