

CYBER INSURANCE ENDORSEMENT

(Event Discovered and Reported First Party Coverage)

NOTICE

This Endorsement (“Endorsement”) amends the Professional Liability Policy (“the policy”) issued by Lawyers’ Mutual Insurance Company (“Company”) to provide first-party Cyber Insurance on an Event Discovered and Reported basis. This Endorsement does not alter or change the terms and conditions of the policy.

Written notice of an **insured event** must be reported pursuant to the terms of Section V of this Endorsement. Notice shall be given to the Company via NAS Insurance Services, LLC at:

NAS Insurance Services, LLC
16501 Ventura Blvd., Suite 200
Encino, CA 91436
(T): (818) 382-2030
(F): (818) 382-2040
claims@nasinsurance.com

NOTICE OF AN INSURED EVENT UNDER THIS ENDORSEMENT SHALL NOT BE DEEMED TO CONSTITUTE NOTICE OF A CLAIM OR POTENTIAL CLAIM UNDER THE POLICY TO WHICH THIS ENDORSEMENT IS ATTACHED.

Various provisions in this Endorsement restrict coverage. Read the entire Endorsement carefully to determine the **insured’s** rights and duties and what is and is not covered. The terms, conditions, exclusions, and limits of insurance set forth in this Endorsement apply only to the coverage provided by this Endorsement.

COVERAGE HEREUNDER EXPIRES ON THE EXPIRATION DATE OF THE POLICY OR ON ITS EARLIER CANCELLATION OR NON-RENEWAL DATE. NO EXTENDED REPORTING PERIOD IS AVAILABLE FOR THE COVERAGE UNDER THIS ENDORSEMENT.

All words and phrases in this Endorsement that appear in bold print have the meanings set forth in Section I of this Endorsement. To the extent any words or phrases used in this Endorsement are defined elsewhere in the policy, such definitions provided elsewhere do not apply to or give meaning to the words or phrases used in this Endorsement.

The limits of Cyber Insurance are specified in the Schedule of Limits (“Schedule”) shown below. Such limits of insurance are in addition to, and will not erode, the limits of liability of the policy set forth in the Company’s Declarations.

SCHEDULE OF COVERAGE AGREEMENTS AND LIMITS

Coverage Agreements	Limits
Privacy Breach Response Costs, Notification Expenses and Breach Support and Credit Monitoring Expenses Coverage	\$100,000 each insured event \$100,000 aggregate limit
Network Asset Protection Coverage	
Cyber Extortion Coverage	

IMPORTANT

The Endorsement contained herein does not become effective unless a DECLARATIONS insert (“Declarations”) is issued to form a part hereof.

SECTION I - DEFINITIONS

Whenever used in this Endorsement:

Adverse media report means any report or communication of an actual or potential **security breach** or **privacy breach**, which:

- A. Has been publicized through any media channel including, but not limited to, television, **print media**, radio or electronic networks, the **internet**, and/or electronic mail; and
- B. Threatens material damage to the **insured's reputation**.

BPO service provider means any third party independent contractor that provides business process outsourcing services for the **insured's** benefit under a written contract with the **insured**, including, but not limited to, call center services, fulfillment services, and logistical support.

Breach support and credit monitoring expenses means those reasonable and necessary expenses which the **insured** incurs, with the Company's prior written consent, for the provision of support activity to affected persons or organizations, including corporate clients, in the event of a **privacy breach**. For purposes of this definition, "support activity" includes the provision of credit file monitoring services and identity theft education and assistance for up to a period of twelve (12) months from the date of enrollment in such services.

Computer hardware means the physical components of any **computer system** including CPUs, memory, storage devices, storage media, and input/output devices and other peripheral devices and components, including, but not limited to, cable, connectors, fiber optics, wire, power supply units, keyboards, display monitors, and audio speakers.

Computer program means an organized set of instructions that, when executed, causes a computer to behave in a predetermined manner. **Computer program** includes, but is not limited to, communications, networking, operating system, and related **computer programs** used to create, maintain, process, retrieve, store, and/or transmit electronic **data**.

Computer system means interconnected electronic, wireless, web, or similar systems (including all **computer hardware** and software) used to process and store **data** or information in an analogue, digital, electronic, or wireless format including, but not limited to, **computer programs**, electronic **data**, operating systems, **firmware**, servers, media libraries, associated input and output devices, mobile devices, networking equipment, websites, extranets, off line storage facilities (to the extent that they hold electronic **data**), and electronic backup equipment.

Covered cause of loss means, and is limited to, the following:

- A. Accidental Damage or Destruction
 - (1) Accidental physical damage or destruction of **electronic media** so that stored **digital assets** are no longer machine-readable;
 - (2) Accidental physical damage or destruction of **computer hardware** so that stored **data** is no longer machine-readable;
 - (3) Failure in power supply or under/over voltage only if such power supply, including back-up generators, is under the **insured's** direct operational control;
 - (4) **Programming error of delivered programs**; or
 - (5) Electrostatic build-up and static electricity.
- B. Administrative or Operational Mistakes

An accidental, unintentional, or negligent act, error or omission by an **insured**, a **BPO service provider**, or **outsourced IT service provider** in:

- (1) The entry or modification of the **insured's** electronic **data**, which causes damage to such **data**; or
- (2) The creation, handling, development, modification, or maintenance of **digital assets**; or

- (3) The ongoing operation or maintenance of an **insured computer system** excluding the design, architecture, or configuration of an **insured computer system**.

C. Computer Crime and Computer Attacks

An act, mistake or negligent error or omission in the operation of an **insured computer system** or in the handling of **digital assets** by an **insured**, a **BPO service provider**, or **outsourced IT service provider**, which fails to prevent or hinder any of the following on an **insured computer system**:

- (1) A **denial of service attack**;
- (2) **Malicious code**;
- (3) **Unauthorized access**; or
- (4) **Unauthorized use**.

Cyber extortion expenses means all reasonable and necessary costs and expenses which the **insured** incurs, with the Company's prior written consent, as a direct result of a **cyber extortion threat**, other than **cyber extortion monies**.

Cyber extortion monies means any funds or property which the **insured** pays, with the Company's prior written consent, to a person(s) or entity(ies) reasonably believed to be responsible for a **cyber extortion threat**, for the purpose of terminating such **cyber extortion threat**.

Cyber extortion threat means a credible threat or series of related credible threats, including, but not limited to, a demand for **cyber extortion monies**, directed at an **insured** to:

- A. Release, divulge, disseminate, destroy or use the confidential information of a third party taken from the **insured** as a result of **unauthorized access** to, or **unauthorized use** of, an **insured computer system**;
- B. Introduce **malicious code** into an **insured computer system**;
- C. Corrupt, damage or destroy an **insured computer system**;
- D. Restrict or hinder access to an **insured computer system**, including, but not limited to the threat of a **denial of service attack**; or
- E. Electronically communicate with the **insured's** clients and falsely claim to be the **insured** or to be acting under the **insured's** direction in order to falsely obtain personal or confidential information of the **insured's** clients (also known as "pharming," "phishing," or other types of false communications).

Data means any and all machine-readable information, including, but not limited to, ready-for-use programs, applications, account information, personal information, health and medical information, or electronic information subject to back-up procedures, irrespective of the way it is used and rendered.

Delivered programs means programs, applications, and software where the development stage has been finalized, having passed all test-runs, and been proven successful in a live environment.

Denial of service attack means an event caused by unauthorized or unexpected interference or a malicious attack intended by the perpetrator to overwhelm the capacity of a **computer system** by sending an excessive volume of electronic **data** to such **computer system** in order to prevent authorized access to such **computer system**.

Digital assets means **data** and **computer programs** that exist in an **insured computer system**. **Digital assets** do not include **computer hardware**.

Digital assets loss means reasonable and necessary expenses and costs which the **insured** incurs to replace, recreate, or restore **digital assets** to the same state and with the same contents immediately before it was damaged, destroyed, altered, misused, or stolen, including expenses for materials and machine time. **Digital assets loss** will be determined as follows:

- A. If the impacted **digital asset** was purchased from a third party, the Company will pay only the lesser of the original purchase price of the **digital asset** or the reasonable and necessary **digital assets loss**.
- B. If it is determined that the **digital assets** cannot be replaced, restored or recreated, then the Company will only reimburse the actual and necessary **digital assets loss** incurred up to such determination.

Electronic media means floppy disks, CD ROMs, hard drives, magnetic tapes, magnetic discs, or any other media on which electronic data is recorded or stored.

Endorsement effective date means the date listed as such on this Endorsement.

Endorsement period means the period of coverage commencing on the **endorsement effective date** and ending on the earlier of the termination, expiration or cancellation date of the policy to which this Endorsement attaches. **Endorsement period** does not include the time period set forth in any Extended Reporting Period Endorsement issued by the Company.

Firmware means the fixed programs that internally control basic low-level operations in a device.

Insured means the **named insured**. **Insured** also means any persons who qualify as “insureds” under the policy, but only while such persons are acting within the scope of their duties on behalf of the **named insured**.

Insured computer system means:

- (1) A **computer system** operated by and either owned by, or leased to, the **named insured**;
- (2) With respect to Coverage Agreement B only, a **computer system** operated by a **BPO service provider** or **outsourced IT service provider** and used for the sole purpose of providing hosted computer application services to the **insured** or for processing, maintaining, hosting, or storing electronic **data** on behalf of the **insured**, pursuant to a written contract with the **insured** for such services.

Insured event means:

- A. With respect to Coverage Agreement A (Privacy Breach Response Costs, Notification Expenses, and Breach Support and Credit Monitoring Expenses), an **adverse media report**, **security breach**, or **privacy breach**.
- B. With respect to Coverage Agreement B (Network Asset Protection), a **covered cause of loss**.
- C. With respect to Coverage Agreement C (Cyber Extortion), a **cyber extortion threat**.

Insured event only pertains to loss sustained by the **insured** and does not include any demand, allegation or lawsuit made or brought by or on behalf of any third party.

Insured's reputation means the estimation of trust that clients have in doing business with the **insured** or in retaining the **insured's** services.

Internet means the worldwide public network of computers which enables the transmission of electronic **data** between different users, including a private communications network existing within a shared or public network platform.

Malicious code means software intentionally designed to insert itself and damage a **computer system** without the owner's informed consent by a variety of forms including, but not limited to, virus, worm, Trojan horses, spyware, dishonest adware, and crimeware.

Named insured means the partnership, professional corporation or individual named as such on the Company's Declarations.

Notification expenses means:

- A. Those reasonable and necessary legal expenses, computer forensic and investigation fees, public relations expenses, postage expenses and related advertising expenses incurred by the **insured**, with the Company's prior written consent, to comply with governmental privacy legislation mandating notification to affected individuals in the event of a **security breach** or **privacy breach**; and
- B. **Voluntary notification expenses** incurred with the Company's prior written consent.

Operational programs means programs and software which are ready for operational use, having been fully developed, tested, and accepted by the **insured**.

Outsourced IT service provider means a third party independent contractor that provides information technology services for the **insured's** benefit under a written contract with the **insured**. **Outsourced IT service provider** services include, but are not limited to, hosting, security management, co-location, and **data** storage.

Print media means newspapers, newsletters, magazines, books, and literary works in any form, brochures or other types of publications, and advertising materials, including packaging, photographs, and digital images.

Privacy breach means any of the below, whether actual or alleged, but only if committed or allegedly committed by an **insured**, or by others acting on the **insured's** behalf and for whom the **insured** is legally responsible, including **BPO service providers** and **outsourced IT service providers**:

- A. The unauthorized collection, disclosure, use, access, destruction or modification of private information, or the inability to access, or failure to provide, private information;
- B. The surrender of private information as a result of false communications or social engineering techniques including but not limited to phishing, spear-phishing, and pharming;
- C. Any breach of privacy regulations, as they currently exist and as amended, associated with the confidentiality, access, control, and use of personally identifiable, non-public information, including, but not limited to:
 - (1) Health Insurance Portability and Accountability Act of 1996 (Public Law 104- 191), known as HIPAA, and related state medical privacy laws;
 - (2) Gramm-Leach-Bliley Act of 1999 (G-L-B), also known as the Financial Services Modernization Act of 1999;
 - (3) State and federal statutes and regulations regarding the security and privacy of consumer information;
 - (4) Governmental privacy protection regulations or laws associated with the control and use of personal information;
 - (5) Privacy provisions of consumer protection laws, including the Federal Fair Credit Reporting Act (FCRA) and similar state laws;
 - (6) Title XIII, the Health Information Technology for Economic and Clinical Health Act ("HITECH"), of the American Recovery and Reinvestment Act of 2009 ("ARRA").

Privacy breach response costs means:

- A. Those reasonable and necessary fees and expenses the **insured** incurs, with the Company's prior written consent, for the employment of a public relations consultant following the publication of an **adverse media report**, if the **insured** reasonably considers such action is necessary in order to avert or mitigate any material damage to the **insured's reputation**, which results or reasonably will result from the **adverse media report**; and
- B. **Proactive privacy breach response costs** incurred with the Company's prior written consent.

Proactive privacy breach response costs means those reasonable and necessary public relations expenses the **insured** incurs, with the Company's prior written consent, in response to an actual or potential **security breach** or **privacy breach**, but prior to the publication of an **adverse media report**, in an effort to avert or mitigate the potential impact of an **adverse media report**.

Programming error means an error which occurs during the development or encoding of a computer program, software, or application, which would, when in operation, result in a malfunction or incorrect operation of a **computer system**.

Property damage means injury to tangible property, including all resulting loss of use of that property, and loss of use of tangible property that is not physically injured. **Data** is not considered tangible property.

Security breach means any of the following, whether a specifically targeted attack or a generally distributed attack:

- A. **Unauthorized access** to, or **unauthorized use** of, an **insured computer system**, including **unauthorized access** or **unauthorized use** resulting from the theft of a password from an **insured computer system** or from any **insured**;
- B. A **denial of service attack** against an **insured computer system**; or
- C. Infection of an **insured computer system** by **malicious code** or the transmission of **malicious code** from an **insured computer system**,

Special expenses means reasonable and necessary costs and expenses which the **insured** incurs to:

- A. Prevent, preserve, minimize, or mitigate any further damage to **digital assets**, including the reasonable and necessary fees and expenses of specialists, outside consultants, or forensic experts;
- B. Preserve critical evidence of any criminal or malicious wrongdoing;
- C. Purchase replacement licenses for **computer programs** because the copy protection system and/or access control software was damaged or destroyed by a **covered cause of loss**; or
- D. Notify clients of a total or partial interruption, degradation in service, or failure of an **insured computer system** resulting from a **covered cause of loss**.

Unauthorized access means the gaining of access to a **computer system** by an unauthorized person or persons.

Unauthorized use means the use of a **computer system** by unauthorized persons or authorized persons in an unauthorized manner.

Voluntary notification means written notice to any individual or organization of a **privacy breach** or **security breach** where there is no specific legal requirement in the applicable jurisdiction mandating such notice.

Voluntary notification expenses means reasonable and necessary legal expenses, computer forensic and investigation fees, public relations expenses, postage expenses and related advertising expenses incurred by the **insured**, with the Company's prior written consent, as a result of **voluntary notification**.

SECTION II – CYBER INSURANCE COVERAGE

In consideration of the premium paid and subject to all terms, conditions, definitions, exclusions and other provisions of this Endorsement, the Company agrees as follows:

A. PRIVACY BREACH RESPONSE COSTS, NOTIFICATION EXPENSES, AND BREACH SUPPORT AND CREDIT MONITORING EXPENSES COVERAGE

Subject to the limits shown in the Schedule, the Company will pay reasonable **privacy breach response costs**, **notification expenses**, and **breach support and credit monitoring expenses** which the **insured** incurs after the **endorsement effective date** as a direct result of an **adverse media report**, **security breach** or **privacy breach**, provided that:

- (1) The **adverse media report**, **security breach** or **privacy breach** takes place or first commences on or after the **endorsement effective date**;
- (2) The **adverse media report**, **security breach** or **privacy breach** is first discovered by the **insured** during the **endorsement period**; and
- (3) The **adverse media report**, **security breach** or **privacy breach** is reported to the Company no later than 60 days from the date the **insured** first discovers the **adverse media report**, **security breach** or **privacy breach**.

The **insured** shall not pay **privacy breach response costs**, **notification expenses**, or **breach support and credit monitoring expenses** without the Company's prior consultation and written authorization.

B. NETWORK ASSET PROTECTION COVERAGE

Subject to the limits shown in the Schedule, the Company will reimburse the **insured** for **digital assets loss** and **special expenses** which the **insured** incurs after the **endorsement effective date** as a direct result of damage, alteration, corruption, distortion, theft, misuse, or destruction of **digital assets**, provided that:

- (1) Such damage, alteration, corruption, distortion, theft, misuse, or destruction of **digital assets** is directly caused by a **covered cause of loss** that takes place or first commences on or after the **endorsement effective date**;
- (2) The **covered cause of loss** is first discovered by the **insured** during the **endorsement period**;
- (3) The **covered cause of loss** is reported to the Company no later than 60 days from the date the **insured** first discovers the **covered cause of loss**.

The **insured** shall not pay **digital assets loss** or **special expenses** without the Company's prior consultation and written authorization. The Company will pay **digital assets loss** and **special expenses** for a period of up to twelve (12) months following the discovery of the damage, alteration, corruption, distortion, theft, misuse, or destruction of **digital assets**.

C. CYBER EXTORTION COVERAGE

Subject to the limits shown in the Schedule, the Company will reimburse the **insured** for **cyber extortion expenses** incurred and **cyber extortion monies** paid after the **endorsement effective date** as a direct result of a **cyber extortion threat**, including a demand for **cyber extortion monies**, provided that:

- (1) Such **cyber extortion threat** is first made against the **insured** during the **endorsement period**;
- (2) The **cyber extortion expenses** and **cyber extortion monies** directly resulted from the **cyber extortion threat**; and
- (3) The **cyber extortion threat** is reported to the Company no later than 60 days from the date the **cyber extortion threat** is made against the **insured**.

The **insured** shall not pay **cyber extortion expenses** or **cyber extortion monies** without the Company's prior consultation and written authorization. The **insured** must make every reasonable effort to notify local law enforcement authorities and the Federal Bureau of Investigation, or similar equivalent foreign agency, before surrendering any **cyber extortion monies** in response to a **cyber extortion threat**.

SECTION III – CYBER INSURANCE EXCLUSIONS

This Endorsement does not apply to:

A. Any **insured event**:

- (1) Which was the subject of written notice given to the Company or to any other insurer prior to the **endorsement effective date**; or
- (2) Which an **insured** had knowledge of prior to the **endorsement effective date**.

B. Any loss which is covered under the policy to which this endorsement is attached.

C. **Property damage**.

D. Any **insured event** based upon, arising out of, resulting from, in consequence of, or in any way involving:

- (1) Satellite failures;
- (2) Electrical or mechanical failures or interruption including, but not limited to, electrical disturbance, spike, brownout, or blackout;
- (3) Outages to gas, water, telephone, cable, telecommunications or other infrastructure, unless such

infrastructure is under the **insured's** direct operational control and such **insured event** is otherwise covered under Coverage Agreement B;

- (4) The failure of overhead transmission and distribution lines;
- (5) The gradual deterioration of subterranean insulation; or
- (6) The existence, emission or discharge of any electromagnetic field, electromagnetic radiation or electromagnetism.

E. Any **insured event** based upon, arising out of, resulting from, in consequence of, or in any way involving any of the following, if committed by any person with ownership interest in the **named insured**, whether acting alone or in collusion with other persons:

- (1) Any willful, deliberately dishonest, malicious, or fraudulent act or omission;
- (2) Any intentional violation of the law or of the **named insured's** privacy policy;
- (3) The gaining in fact of any profit, remuneration or financial advantage to which the **insured** was not legally entitled.

F. Any **insured event** based upon, arising out of, resulting from, in consequence of, or in any way involving any business, joint venture or enterprise of an **insured** which is not named on the Company's Declarations.

G. Any **insured event** based upon, arising out of, resulting from, in consequence of, or in any way involving any conduct, act, error or omission of any **insured** serving in any capacity other than as the **named insured's** officer, director, partner, stockholder, trustee or employee.

H. Any **insured event** based upon, arising out of, resulting from, in consequence of, or in any way involving:

- (1) The wear and tear, drop in performance, progressive deterioration, or aging of the **insured's** electronic equipment or **computer hardware**; or
- (2) The gradual deterioration or wear and tear of an **insured computer system**.

I. Any **insured event** based upon, arising out of, resulting from, in consequence of, or in any way involving fire, smoke, explosion, lightning, wind, water, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, force majeure or any other physical event, however caused.

J. Any **insured event** based upon, arising out of, resulting from, in consequence of, or in any way involving:

- (1) The confiscation, nationalization, commandeering, requisition or destruction of, or damage to, **computer hardware** or other property by order of a public or local authority, government de jure or government de facto for whatever reason;
- (2) Strikes or similar labor actions, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular uprising, military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions; or
- (3) Any action taken in controlling, preventing, suppressing or in any way relating to J(1) or J(2) above.

K. Any **insured event** based upon, arising out of, resulting from, in consequence of, or in any way involving the use of programs that are not **operational programs** or **delivered programs**.

L. Any **insured event** based upon, arising out of, resulting from, in consequence of, or in any way involving any **insured's** intentional use of illegal or unlicensed programs that are in violation of the provisions or laws referring to software protection.

M. Physical damage to **computer hardware** or **data center**, other than accidental physical damage or destruction of **electronic media** so that stored **digital assets** are no longer machine-readable.

N. Any obligation to reimburse or indemnify third parties for whatever reason.

- O. Fines or penalties imposed by law.
- P. The economic or market value of **digital assets**.
- Q. Costs or expenses incurred to identify, patch or remediate software program errors or **computer system** vulnerabilities.
- R. Costs to upgrade, redesign, reconfigure or maintain an **insured computer system** to a level of functionality beyond that which existed prior to the **covered cause of loss**; or costs to restore, update or replace **digital assets** to a level beyond that which existed prior to the **covered cause of loss**.
- S. Loss of revenue resulting from an **insured event**.

SECTION IV – CYBER INSURANCE LIMITS

- A. The “each **insured event**” limit shown in the Schedule is the most the Company will pay for each **insured event**, regardless of the number of **insureds** involved or affected.
- B. The “aggregate limit” shown in Schedule is the most the Company will pay for loss arising from any and all **insured events** for which coverage attaches under this Endorsement, regardless of the number of **insureds** involved or affected or the number of **insured events**. The “aggregate limit” is shared with all **insureds**.
- C. If the “aggregate limit” is exhausted, then the Company’s obligations under this Endorsement will be deemed completely fulfilled and extinguished. The Company’s obligations under this Endorsement will not be affected by the exhaustion of the Professional Liability Aggregate Limit of the policy to which this Endorsement is attached.
- D. All **insured events** arising out of the same, related, repeated or continuing acts, facts, circumstances incidents or events, will be considered a single **insured event**. Such **insured event** will be deemed to have been first reported to the Company on the date the first of the related **insured events** was reported to the Company. **Insured events** will be deemed related if the Company determines that they are logically or causally connected by any common fact, circumstance, situation, event, transaction or series of facts, circumstances, situations, events or transactions.

SECTION V – CYBER INSURANCE NOTICE PROVISIONS

- A. As a condition precedent to coverage under this Endorsement, the **insured** must give the Company written notice of any **insured event** no later than 60 days from the date the **insured** first discovers the **insured event**.
- B. Written notice shall be given to the Company via NAS Insurance Services, LLC at:

NAS Insurance Services, LLC
16501 Ventura Blvd., Suite 200
Encino, CA 91436
(T): (818) 382-2030
(F): (818) 382-2040
claims@nasinsurance.com

The **insured** must provide NAS Insurance Services, LLC with supporting documentation as well as any authorization, cooperation, or assistance required.

- C. The Company will not be obligated to pay any amounts incurred prior to notice of an **insured event** to the Company or amounts incurred without the Company’s prior written consent.
- D. Notice of an **insured event** under this Endorsement shall not be deemed to constitute notice of a claim or potential claim under the Professional Liability policy to which this Endorsement is attached.