PROFESSIONAL LIABILITY

# MARKEL INSURANCE COMPANY

**THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.**

## BREACH MITIGATION EXPENSE, RANSOMWARE ATTACK AND WIRE FRAUD COVERAGE

This endorsement modifies insurance provided under the following:

LAWYERS PROFESSIONAL LIABILITY INSURANCE POLICY

This policy is amended as follows:

**SCHEDULE**

**Breach Mitigation Expense**, **Ransomware Attack** and **Wire Fraud Limits of Liability**

| | | |
|---|---|---|
| **Breach Mitigation Expense**: Each **Unintentional Data Compromise** | $ | 25,000 |
| **Ransomware Attack**: Each **Ransomware Attack** | $ | 25,000 |
| **Wire Fraud**: Each **Loss** | $ | 25,000 |
| **Breach Mitigation Expense**, **Ransomware Attack** and **Wire Fraud** Aggregate | $ | 25,000 |

**A.** SECTION I – COVERAGE, B. Supplementary Payments is amended by the addition of the following:

**4. Breach Mitigation Expense Coverage – Occurrence Coverage:**

The Company shall reimburse the **Named Insured** up to the amount stated in the **Breach Mitigation Expense**, **Ransomware Attack** and **Wire Fraud** Limits of Liability Schedule as applicable to **Breach Mitigation Expense** for the reasonable cost actually incurred by the **Named Insured** for **Breach Mitigation Expense**, subject to the prior written consent of the Company, which results directly from each **Unintentional Data Compromise** which occurs during the **Policy Period** and is reported to the Company pursuant to the **Breach Mitigation Expense**, **Ransomware Attack** and **Wire Fraud** Reporting and Payment Provision, provided:

**a.** The entirety of the **Unintentional Data Compromise** occurs during the **Policy Period**; and

**b.** Prior to the effective date of this policy the **Named Insured** or any past or current principal, partner, officer, director, trustee, shareholder or employee of the **Named Insured** had no knowledge that such **Unintentional Data Compromise** of:

**i.** The **Named Insured's Electronic Communications System**; or

**ii.** The **Electronic Communications System** of a third party responsible for storing and securing the data of the **Named Insured**;

Had occurred in whole or in part which may have led a reasonable person in such party's position to conclude that incurring such expenses was likely, and if any such party knew prior to the **Policy Period** that such **Unintentional Data Compromise** had occurred, then any continuation, change or resumption of such **Unintentional Data Compromise** during or after the **Policy Period** will be deemed to have been known prior to the **Policy Period**; and

**c.** **Unintentional Data Compromise** will be deemed to have been known to have occurred at the earliest of any **Insured**:

**i.** Reporting all, or any part, of an **Unauthorized Access** to the Company, any other insurer or any insurance representative;

**ii.** Incurring **Breach Mitigation Expense** because of an **Unauthorized Access**; or

**iii.** Becoming aware by any other means that an **Unintentional Data Compromise** has occurred or has begun to occur.

The **Named Insured** must submit to the Company a Sworn Proof of Loss of such costs within one (1) year after the expiration or cancellation of this policy.

**5. Ransomware Attack Coverage – Occurrence Coverage:**

The Company shall reimburse the **Named Insured** up to the amount stated in the **Breach Mitigation Expense**, **Ransomware Attack** and **Wire Fraud** Limits of Liability Schedule as applicable to **Ransomware Attack** for **Loss** arising directly from each **Ransomware Attack** which occurs during the **Policy Period** and is reported to the Company pursuant to the **Breach Mitigation Expense**, **Ransomware Attack** and **Wire Fraud** Reporting and Payment Provision, provided:

**a.** The entirety of the **Ransomware Attack** occurs during the **Policy Period**; and

**b.** Prior to the effective date of this policy the **Named Insured** or any past or current principal, partner, officer, director, trustee, shareholder or employee of the **Named Insured** had no knowledge that such **Ransomware Attack** had occurred in whole or in part which may have led a reasonable person in such party's position to conclude that incurring **Loss** was likely, and if any such party knew prior to the **Policy Period** that such **Ransomware Attack** had occurred, then any continuation, change or resumption of such **Ransomware Attack** during or after the **Policy Period** will be deemed to have been known prior to the **Policy Period**; and

**c.** **Ransomware Attack** will be deemed to have been known to have occurred at the earliest of any **Insured**:

**i.** Reporting all, or any part, of a **Ransomware Attack** to the Company, any other insurer or any insurance representative;

**ii.** Incurring **Loss** or **Breach Mitigation Expenses** because of the **Ransomware Attack**; or

**iii.** Becoming aware by any other means that a **Ransomware Attack** has occurred or has begun to occur.

**6. Wire Fraud Coverage – Occurrence Coverage:**

The Company shall reimburse the **Named Insured** up to the amount stated in the **Breach Mitigation Expense**, **Ransomware Attack** and **Wire Fraud** Limits of Liability Schedule as applicable to **Wire Fraud** for **Loss** incurred by the **Named Insured** arising directly from each **Wire Fraud** which occurs during the **Policy Period** and is reported to the Company pursuant to the **Breach Mitigation Expense**, **Ransomware Attack** and **Wire Fraud** Reporting and Payment Provision, provided:

**a.** The entirety of the **Wire Fraud** occurs during the **Policy Period**;

**b.** Prior to the effective date of this policy the **Named Insured** or any past or current principal, partner, officer, director, trustee, shareholder or employee of the **Named Insured** had no knowledge that such **Wire Fraud** had occurred in whole or in part which may have led a reasonable person in such party's position to conclude that incurring **Loss** was likely, and if any such party knew prior to the **Policy Period** that such **Wire Fraud** had occurred, then any continuation, change or resumption of such **Wire Fraud** during or after the **Policy Period** will be deemed to have been known prior to the **Policy Period**; and

**c.** **Wire Fraud** will be deemed to have been known to have occurred at the earliest of any **Insured**:

**i.** Reporting all, or any part, of a **Wire Fraud** to the Company, any other insurer or any insurance representative; or

**ii.** Becoming aware by any other means that a **Wire Fraud** has occurred or has begun to occur.

**7. Breach Mitigation Expense, Ransomware Attack** and **Wire Fraud Aggregate** Limit:

The amount stated in the **Breach Mitigation Expense**, **Ransomware Attack** and **Wire Fraud** Limit of Liability Schedule as Aggregate shall be the Company's maximum aggregate liability for the total of all **Breach Mitigation Expense**, **Loss** arising from **Ransomware Attack** and **Loss** arising from **Wire Fraud** coverage.

**8. Breach Mitigation Expense**, **Ransomware Attack** and **Wire Fraud** Reporting and Payment Provision:

**a.** Reporting Provision:

It is a condition precedent to coverage afforded by Supplementary Payments Items 4. - 7. that the **Insured** shall give to the Company written notice, as soon as practicable and in no event later than ninety (90) days after the end of the **Policy Period**, of any **Unintentional Data Compromise**, **Ransomware Attack** or **Wire Fraud** which occurs during the **Policy Period**.

The **Insured** must:

**i.** Take all reasonable steps to protect the **Named Insured's Electronic Communications System** from further **Unauthorized Access**, if applicable;

**ii.** Notify law enforcement in the event of a theft;

**iii.** As soon as practicable, provide a description of how, when and what elements, if any, of the **Named Insured's** or a third party's **Electronic Communications System** were impacted by the **Unintentional Data Compromise** or **Unauthorized Access**;

**iv.** As soon as practicable, provide a description of how, when and where the **Wire Fraud** occurred;

**v.** Submit to the Company a Sworn Proof of Loss of such **Breach Mitigation Expenses** within one (1) year after the expiration or cancellation of this policy; and

**vi.** As often as may be reasonably required, permit the Company to inspect the **Named Insured's Electronic Communications System** and examine the **Insured's** books and records related to the **Breach Mitigation Expense** or **Loss** incurred.

**b.** Payment Provision:

The Company may, at its sole discretion, investigate any **Breach Mitigation Expense**, any **Unintentional Data Compromise,** any **Unauthorized Access**, any **Ransomware Attack** or any **Wire Fraud**.

The Company will indemnify the **Named Insured** within sixty (60) days after it receives a Sworn Proof of Loss of **Breach Mitigation Expenses** or **Loss**, provided:

**i.** The **Insured** has complied with all the terms of this coverage; and

**ii.** The Company and the **Named Insured** have agreed with the items included within and the amounts documented in the **Named Insured's** Sworn Proof of Loss of **Breach Mitigation Expenses** or **Loss**.

**9. Breach Mitigation Expense, Ransomware Attack** and **Wire Fraud** Exclusions:

**a.** With respect to the coverage afforded by Supplementary Payments Items 4. - 8., the Company shall not be liable to pay any **Breach Mitigation Expense** or **Loss**:

**i.** Caused by any government, governmental agency or sub-agency, or any agents thereof while acting on behalf of such entity;

**ii.** Due to riot, civil commotion, war, insurrection or usurped power;

**iii.** Any act, error or omission in the performance of **Professional Services** rendered or that should have been rendered by the **Insured** or by any person or organization for whose acts, errors or omissions the **Insured** is legally responsible. However, this exclusion shall not apply to **Loss** arising from **Wire Fraud;**

**iv.** Any violation of any antitrust law;

**v.** Caused by conduct of the **Insured** or at the **Insured's** direction that is intentional, willful, dishonest, fraudulent or that constitutes a willful violation of any statute or regulation; provided, however, this exclusion shall not apply to the strictly vicarious liability of any **Insured** for the intentional, willful, dishonest or fraudulent conduct of another **Insured** or for the conduct of another **Insured** that constitutes a willful violation of any statute or regulation;

**vi.** Based upon, arising out of, or in any way involving any fact, circumstance, **Unintentional Data Compromise, Unauthorized Access, Ramsomware Attack** or **Wire Fraud** which have been the subject of any written notice given prior to inception of this policy under any prior insurance policy or coverage part;

**vii.** For which amounts coverage provided by any other coverage provided elsewhere in this policy. No coverage is provided for **Breach Mitigation Expense**, or **Loss** caused by **Ransomware Attack** or **Wire Fraud** under this policy, except as provided by Supplementary Payments Items 4. - 8.; or

**viii.** Arising out of **Electronic Media Injury**.

**b.** With respect to **Ransomware Attack**, this insurance does not apply to any **Loss**:

**i.** Caused by theft, physical damage or destruction of the **Named Insured's Electronic Communications System** or any part thereof. However, this exclusion does not apply to destruction of programs, **Electronic Data** and media caused by an **Unauthorized Access**; or

**ii.** Of the value of trade secrets, confidential processing methods or other confidential or proprietary information.

**c.** With respect to **Wire Fraud**, this insurance does not apply to any **Loss**:

**i.** Resulting directly or indirectly from:

**(a)** Failure to verbally contact the **Insured's** client at a prearranged number to verify the request for the wire transfer was sent by the client;

**(b)** Failure to use the prearranged phone number previously provided in the client file, not the phone number in any **Fraudulently Written Electronic Communication**; or

**(c)** Sending pre-filled copies of wire instructions via email without verbally confirming the request came from the **Insured's** actual client;

**ii.** Resulting from mechanical failure, faulty construction, error in design, latent defect, wear and tear, gradual deterioration, electrical disturbance, electronic media failure or breakdown or any malfunction or error in programming or error or omission in processing;

**iii.** Resulting directly or indirectly from the input of **Electronic Data** at an authorized electronic terminal of an electronic funds transfer system or a client computer system by a person who had authorized access from a client to that client's authentication mechanism; or

**iv.** Misuse of confidential information, material or data.

**10. Breach Mitigation Expense, Ransomware Attach** and **Wire Fraud** Definitions:

**a.** When used in this endorsement:

**i. Breach Mitigation Expense** means expenses incurred by the **Named Insured** with the prior written consent of the Company for:

**(a)** The services of a public relations professional, or other publicity expenses that are recommended by a public relations professional to respond to any actual adverse publicity in the media, that is the result of an **Unauthorized Access**;

**(b)** Expenses, including but not limited to, notification and related legal fees that are incurred to comply with a **Security Breach Notice Law** and that are the result of an **Unauthorized Access**; and

**(c)** Expenses associated with voluntarily providing credit monitoring services to individuals effected by an **Unauthorized Access**.

**ii. Electronic Communications System** means any wired, wireless, radio, electromagnetic, photo-optical or photo-electronic facility for the transmission of electronic communications; any **Electronic Data** processing system, network or related electronic equipment for the storage of such communications; and any computer.

**iii. Electronic Data** means facts or information converted to a form usable in an **Electronic Communications System** and which is stored for use by computer programs.

**iv. Electronic Media Injury** means injury arising directly out of the content of the **Named Insured's** website or intranet and caused by or resulting from any of the following offenses:

**(a)** Libel, slander, defamation or any other form of disparagement;

**(b)** Invasion of or infringement of the right of privacy or the right of publicity;

**(c)** Infringement of copyright service mark, service name or trademark, title, trade dress, trade name or slogan and unfair competition alleged in connection therewith;

**(d)** Plagiarism, piracy or misappropriation of ideas under implied contract; or

**(e)** Infliction of emotional distress, mental anguish, false arrest or malicious prosecution.

**v.** **Forensic Expense** means reasonable and necessary costs incurred by the **Named Insured** to engage the services of a third party computer security expert to determine the existence and cause of any **Unauthorized Access**.

**vi.** **Forged** means the signing of the name or electronic manipulation of the name of another natural person with the intent to deceive, but does not mean a signature which consists in whole or in part of one's own name or of any **Insured**, with or without authority, in any capacity for any purpose.

**vii.** **Fraudulently Written Electronic Communication** means an email or other electronic communication fraudulently declared to have been sent by a client, but which was not sent by such client, or was **Forged**, or was fraudulently modified either during physical transit of electronic media to the **Insured** or during electronic transmission to the **Named Insured's Electronic Communications System**.

**viii.** **Loss**:

**1.** Means:

**(a)** Loss of money which is proximately caused by **Ransomware Attack** or by **Wire Fraud;**

**(b)** **Forensic Expense** and other reasonable and necessary costs incurred by the **Named Insured** to restore with due diligence and dispatch the **Named Insured's Electronic Communications System** to the condition that existed prior to an **Unauthorized Access**, including reconstruction of programs, **Electronic Data** and media which form a part of the **Named Insured's Electronic Communications System**.

**2.** Includes, subject to the Company's approval:

**(a)** Necessary expenses incurred by the **Named Insured** to reduce **Loss** after an **Unauthorized Access** or a **Wire Fraud** has happened, but only to the extent that such expenses do not exceed the value of the **Loss** which such expenses are incurred to reduce; and

**(b)** The **Named Insured's** payment of an extortion demand.

**3.** Does not include:

**(a)** Any cost or charges associated with building, modifying or upgrading the **Named Insured's Electronic Communications System**, or any software, security measures or procedures;

**(b)** Any cost required to repair, build or modify tangible property to comply with any award or order by a court, an authority which is charged with the administration or enforcement of laws or regulations relating to the use, transfer or storage of electronic communication or data storage systems, arbitration or any similar proceeding;

**(c)** The **Named Insured's** loss of reputation or client confidence, or the value imputed to such loss;

**(d)** Expenses incurred by the **Named Insured** in establishing the amount of any **Loss** covered under this endorsement;

**(e)** Loss of business income or tax revenue; or

**(f)** Any reduction in the value of trade secrets, confidential processing methods or other confidential or proprietary information.

**ix.** **Private Data** means data containing an individual's:

**1.** Drivers license or other state-issued identification number; social security number; unpublished telephone number; savings account, checking account, credit card or debit card number each when in combination with the security code, access code, password or pin for such account or card number;

**2.** "Nonpublic personal information" as defined in the Gramm-Leach-Bliley Act of 1999, as amended, and regulations issued pursuant thereto;

3. "Protected healthcare information" as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and regulations issued pursuant thereto, and medical and healthcare information;

4. Private personal information as defined under a **Security Breach Notice Law**; and

5. Private personal information as defined under the law of a country other than the United States, which law is intended to provide for the protection of such private personal information.

**Private Data** does not include any lawfully available data accessible by the general public.

x. **Ransomware Attack** means a demand for money by a computer virus that restricts access, locks or takes control of the **Named Insured's Electronic Communications System** resulting from an **Unauthorized Access**.

All **Loss** arising out of a single **Ransomware Attack** or a series of related **Ransomware Attacks** shall be treated as a single **Ransomware Attack**.

xi. **Security Breach Notice Law** means any law, statute or regulation within the United States of America, its territories or possessions, Puerto Rico or Canada, including the European Union (EU) Data Protection Act of 1995, requiring the **Named Insured** to notify individuals of the compromise or possible compromise of the security of their **Private Data** in the **Insured's** care, custody or control.

xii. **Unauthorized Access** means a breach of the **Named Insured's** security measures, systems, procedures, or stated privacy policy, or any intentional violation, interception, or use or misuse of the **Named Insured's Electronic Communications System**, whether or not for profit or gain, by any person, without the permission, knowledge or ratification of the **Insured**. **Unauthorized Access** also includes:

1. Access to the **Named Insured's Electronic Communications System** that is with the **Insured's** permission where such permission is the result of fraud or deception;

2. Use of the **Named Insured's Electronic Communications System** by a party authorized by the **Insured** to use such system, who does so for an unauthorized purpose;

3. The introduction of programs into the **Named Insured's Electronic Communications System** which contain fraudulent or destructive instructions or code, including any inadvertent transmission of such programs to a third party;

4. A credible threat or an extortion demand received by the **Named Insured** threatening or portending loss, injury or damage to:

**(a)** The **Named Insured's Electronic Communications System**, including programs, **Electronic Data** and media which form a part of the **Named Insured's Electronic Communications System**; or

**(b)** Money, securities, bonds or similar financial instruments, solely to the extent that record of such is maintained in digital or electronic format on the **Named Insured's Electronic Communications System**;

For the purpose of extorting money or other valuable consideration from the **Named Insured.**

xiii. **Unintentional Data Compromise** means any computer security incident, intrusion, breach, compromise, theft, loss or misuse of the **Private Data** of the **Named Insured**.

All **Breach Mitigation Expenses** arising out of a single **Unintentional Data Compromise** or a series of related **Unintentional Data Compromises**, shall be treated as a single **Unintentional Data Compromise**.

xiv. **Wire Fraud** means **Loss** arising out of an **Insured's Professional Services** resulting directly from an **Insured** having authorized or transferred, paid or delivered any funds or debited any account relying on **Fraudulently Written Electronic Communication**.

All **Loss** arising out of a single **Wire Fraud** or a series of related **Wire Frauds**, shall be treated as a single **Wire Fraud**.

11. **Breach Mitigation Expense, Ransomware Attack** and **Wire Fraud** General Conditions:

**a.** The following **MITIGATION** provision shall apply to the coverage afforded by Supplementary Payments Items 4. - 10:

**Mitigation**

It is a condition precedent to coverage that the **Insured** shall not willfully fail to comply with any **Security Breach Notice Law** that the **Insured** may be subject to, by reason of an **Unauthorized Access**.

**B.** SECTION VI – EXCLUSIONS is amended by the addition of the following:

This insurance does not apply to:

Any **Loss** or **Breach Mitigation Expense** as defined in this endorsement arising out of an **Unintentional Data Compromise**, a **Ransomware Attack** or a **Wire Fraud** except as provided for in SECTION I - COVERAGE, B. Supplementary Payments, Items 4. - 11.

All other terms and conditions remain unchanged.