

**ACCOUNTANTS PROFESSIONAL LIABILITY
DATA BREACH AND IDENTITY THEFT ENDORSEMENT**

Named Insured:

Policy No.: _____ **Policy Period:** _____ **to** _____ **Effective Date:** _____

Company: **CPA MUTUAL INSURANCE COMPANY OF AMERICA**
RISK RETENTION GROUP

As of the Effective Date shown above, this Endorsement forms a part of and attaches to the Policy identified above.

In consideration of additional premium, it is hereby AGREED:

- I. Terms in bold face type have only the meaning provided in the Policy or specified in this Policy Endorsement.
- II. Definitions
 - A. **Data Breach Event** means any one or more of the following:
 - i. Circumstances involving **You** unintentional failure to prevent the loss, theft, unauthorized acquisition, unauthorized access or other actual or potential breach or compromising of the security or confidentiality of electronically stored **Personally Identifiable Information**, legally in **You** custody or possession at the time of such breach or compromising and obtained by **You** pursuant to **Your** performance of **Professional Services**, which results in a legal obligation, under applicable local, state or federal law or regulations, to notify the person or persons whose **Personally Identifiable Information** was compromised or potentially compromised of such circumstances.
 - ii. The accidental misdirection of electronic mail or other electronic media, including but not limited to, an intranet, extranet or internet connection.
 - iii. The accidental loss of client information transmitted via electronic media.
 - iv. The accidental introduction of a computer virus to a client's or a third party's data, computer, computer system, or network causing harm or damage to that computer, computer system or network.
 - v. The unintentional allowing of a third party to obtain access to a client's computer, computer system or network, without authorization or that exceeds that third party's authorization.
 - B. **Data Breach Event Services** means **Notification Costs** and **Post Breach Expenses** resulting from a **Data Breach Event** first discovered by **You** during the **Policy Period** and reported to the Company in writing within the **Notice Period**.

- C. **Impacted Persons** means the person or persons, residing within the United States, who must be given notice of a **Data Breach Event** pursuant to applicable local, state or federal law or regulations.
- D. **Notice Period** means the time period in which a **Data Breach Event** must be reported to the Company in order for coverage to exist under this Endorsement. The **Notice Period** shall commence immediately upon **Your** first discovery of the **Data Breach Event** during the **Policy Period** and shall terminate immediately upon whichever of the following events occurs first:
- i. The lapse of one half of any time period specified in applicable local, state or federal law or regulations for providing or issuing notice of a **Data Breach Event** to **Impacted Persons**.
 - ii. The lapse of thirty (30) days following **Your** discovery of the **Data Breach Event**.
 - iii. The end of the **Policy Period**.
- E. **Notification Costs** means and is limited to the reasonable and necessary fees and expenses of a Company approved vendor, incurred by us or by **You** with our prior written consent within one (1) year following **Your** discovery of a **Data Breach Event** covered under this Endorsement, for issuing or assisting with the issuing of legally required notice or notices to **Impacted Persons**.
- F. **Personally Identifiable Information** means any of the following:
- i. Information from which an individual may be identified or contacted, including without limitation, an individual's name, address, telephone number, social security number, account relationships, account numbers, account balances, account histories and password.
 - ii. Information concerning or relating to an individual that could reasonably give rise to or result in fraudulent activity, including without limitation, identity misappropriation or identity theft.
 - iii. Information concerning an individual that would be considered "nonpublic personal information" within the meaning of Title V of the Gramm-Leach Bliley Act of 1999 (Public Law 106-102, 113 Stat. 1338) (as amended) and its implementing regulations.
 - iv. Information concerning an individual that would be considered "protected health information" within the Health Insurance Portability and Accountability Act of 1996 (as amended) and its implementing regulations.
- G. **Post Breach Expenses** means and is limited to reasonable fees and expenses of a Company approved vendor, incurred by us or by **You** with our prior written consent within one (1) year following **Your** discovery of a **Data Breach Event** covered under this Endorsement, to mitigate the effects of the **Data Breach Event** by means of the following approved services only:

- i. Providing **Impacted Persons**, who elect to register with the vendor to receive such services, up to one year of identity protection services and such other benefits as registration with the vendor may confer; and
- ii. Providing **Impacted Persons** identity theft education and information materials.

Nothing herein shall prohibit us from providing other assistance the vendor might reasonably be able to offer that we pre-approve, as an ex-gratia benefit, determined in our sole and absolute discretion.

III. Coverage for **Claims**

If, but only if, coverage is otherwise available under the Policy and all conditions of coverage are satisfied, but Section IV. EXCLUSIONS, Exclusion N. excludes a **Claim** arising from a **Data Breach Event** from coverage, then subject to all the terms, conditions and limitations of this Endorsement and provided that the **Data Breach Event** is first discovered by **You** during the **Policy Period** and reported to us in writing within the **Notice Period**, Section IV. EXCLUSIONS, Exclusion N. shall not exclude such **Claim** from coverage. With respect to any **Claim** which is saved from exclusion and subject to coverage pursuant to this Endorsement, **Claims Expenses** shall include **Data Breach Event Services**. Despite contrary provisions in the Policy, including Section III. LIMITS OF LIABILITY, Paragraph D. Multiple Insureds, **Claims** and Claimants and Section V. POLICY CONDITIONS, Paragraph D.2. Duties in the Event of an **Incident** this Endorsement does not apply to and shall not save from exclusion any **Claim** or **Interrelated Claims** asserted more than two (2) years after the date on which the **Data Breach Event** giving rise to such **Claim** or **Interrelated Claims** was reported to the Company. Under no circumstances, however, shall this Endorsement be deemed to create or provide a basis for coverage to exist under any subsequent Policy or save any **Claim** from being excluded by a subsequent Policy or create or provide a basis for coverage under this Policy apart from any coverage which may exist pursuant to this Endorsement. Section V. POLICY CONDITIONS, Paragraph K. Innocent Insureds, is applicable to this coverage.

IV. Supplemental **Data Breach Event** Coverage

If, but only if, applicable local, state or federal law or regulations provide that the **Named Insured** or an **Affiliated Firm**, and not a third party, is the entity that has legal obligation to notify **Impacted Persons** of a **Data Breach Event** and the **Data Breach Event** is first discovered by **You** during the **Policy Period** and reported to us in writing during the **Notice Period**, then subject to all of the terms, conditions and limitations of this Endorsement we will pay for related **Data Breach Event Services** and the fees and costs charged by an attorney we designate or consent to, if incurred by us or by **You** with our written consent, for legal advice and assistance regarding the **Data Breach Event**. Section V. POLICY CONDITIONS, Paragraph K. Innocent Insureds, is applicable to this coverage.

V. **Incident** Reporting

A **Data Breach Event** shall constitute an **Incident** under the Policy, but a notice of an **Incident** involving a **Data Breach Event** shall include, in addition to the information specified in the Policy, providing the number and identity of the **Impacted Persons** and describing the data elements comprising the **Personally Identifiable Information** involved.

VI. Coverage Sublimit

All coverage provided and amounts payable as a result of the existence of this Endorsement, whether as **Claims Expenses, Damages or Data Breach Event Services**, shall be subject to a \$250,000 aggregate coverage sublimit (the “**Endorsement Sublimit**”), as well as the aggregate limit of coverage provided in Section III. LIMITS OF LIABILITY, Paragraph B. Aggregate (the “**Policy Aggregate Limit**”). All amounts payable by us as a result of the existence of this Endorsement shall be within and not in addition to the **Policy Aggregate Limit**, and shall count towards and reduce the **Policy Aggregate Limit**. Once the **Endorsement Sublimit** has been reached, or if the **Policy Aggregate Limit** is reached, our obligation to make payments as a result of the existence of this Endorsement shall terminate regardless of the number of **Claims** made or **Data Breach Events** reported. All coverage provided by this Endorsement is subject to the deductible provision of Section III. LIMITS OF LIABILITY, Paragraph C. Deductible, and our obligation to make any payments as a result of the existence of this Endorsement is in excess of the applicable deductible amount.

VII. Endorsement Exclusions

This Endorsement does not apply to any of the following:

- A. Any **Claim** or **Data Breach Event** related to, arising out of or resulting from any electrical or mechanical failures, including without limitation: (1) any electrical power interruption, surge, brownout, blackout or other failure; and (2) any failure of telephone lines, data transmission lines, satellites or other infrastructure supporting the Internet.
- B. Any **Claim** or **Data Breach Event** related to, arising out of or resulting from **Your** failure to do any of the following:
 - i. Use, maintain and update at a minimum every ninety (90) days, when necessary, anti-virus software, firewall software on all broadband or high-speed connections to the Internet and software security patches.
 - ii. Comply with all data security standards issued by credit card issuers or financial institutions with whom **You** transact business, if **You** process, store or handle credit card information.

VIII. Except as provided herein, all other terms, conditions, limitations and exclusions of the Policy remain unchanged.

Authorized Representative