

## SUMMARY OF BENEFITS FOR THE MERCHANT DATA SECURITY PROGRAM

This Summary of Benefits is a summary of the terms and conditions of the Merchant Data Security Program (the “**Program**”) administered by Royal Group Services (RGS) on behalf of Trustwave Holdings, Inc.. (**the named insured**) This Summary of Benefits is not an insurance policy or a certificate of insurance. Subject to certain terms and conditions, **Participating merchants** are entitled to the benefits described below.

### GENERAL INFORMATION

Should you have any questions regarding the **Program**, or wish to view a complete copy of the terms and conditions, please visit the web portal ([www.royalgroupservices.com/trustwaveholdings](http://www.royalgroupservices.com/trustwaveholdings)) and view the section “What is the PCI Protection Plan”. If you have additional questions, select the tab “Questions Regarding the Program” to submit your question. Questions will be answered within one business day.

**PROGRAM LIMITS:** \$100,000 per **MID** \$500,000 per **Merchant**

### BENEFIT

Subject to all of the terms, conditions and exclusions set forth below, The named insured shall reimburse, or pay on behalf of, a **participating merchant** for all reasonable **card association assessments, forensic audit expenses, card replacement expenses, and post event services expenses** resulting from any **data security event** discovered while such **participating merchant** is enrolled in the **program**.

To report a **data security event** under the program, visit the web portal ([www.royalgroupservices.com/trustwaveholdings](http://www.royalgroupservices.com/trustwaveholdings)) and view the section “Claims”. Please follow the instructions for submitting a claim.

### DEFINITIONS

**ADCR fines** means amounts contractually assessed against a **merchant** or the **named insured** by a **card association** to cover partial collection of losses experienced by a **bank card** issuer as a result of a **data security event**, including the Account Data Compromise Recovery process and similar processes.

**Bank card** means a financial transaction card, including a debit card, credit card or prepaid card, issued by a **card association** or a financial institution as a member of a **card association**.

**Cardholder** means a natural person or entity to which a **bank card** has been issued.

**Cardholder Information** means the data contained on a **bank card**, or otherwise provided to **you**, that is required to process, approve and/or settle a **bank card** transaction.

**Card association** means each of Visa International, MasterCard Worldwide, Discover Financial Services, JCB, American Express and any similar credit or debit card association that is a participating organization of the PCI Security Standards Council.

**Card association assessment** means a monetary assessment, fee, fine or penalty levied against a **merchant** or the **named insured** by a **card association** as the result of (i) a **data security event** or (ii) a security assessment conducted as the result of a **data security event**. The **card association assessment** shall not exceed the maximum monetary assessment, fee, fine or penalty permitted upon the occurrence of a **data security event** by the applicable rules or agreement in effect as of the inception date of the **policy period** for such **card association**.

**Card replacement expenses** means the costs **you** are required to pay to replace compromised **bank cards** as the result of (i) a **data security event** or (ii) a security assessment conducted as the result of a **data security event**

**Chargeback** means the procedure by which a **bank card** transaction is returned to a **merchant** which is then responsible for the amount of such transaction.

**Compliance case costs** means costs and expenses incurred by a card issuer in monitoring and addressing **bank card** accounts which are reasonably believed to be compromised or at risk as a result of a **data security event** and for which reimbursement is requested pursuant to rules of a **card association**. **Compliance case costs** do not include **chargeback** amounts.

**Data security event** means the actual or suspected unauthorized access to or use of **cardholder information**, arising out of a **merchant’s** possession of or access to such **cardholder information**, which has been reported (a) to a **card association** by a **merchant** or the **named insured** or (b) to the **merchant** or the **named insured** by a **card association**. All **security event expenses** and **post event services expenses** resulting from the same, continuous, related or repeated event or which arise from the same, related or common nexus of facts, will be deemed to arise out of one **data security event**.

**Forensic audit expenses** means the costs of (i) a forensic investigation conducted to determine the cause and extent of a **data security event**, and (ii) a security assessment conducted by a qualified security assessor approved by a **card association** or the PCI Security Standards Council.

**Merchant** means each and every entity that enters into an agreement pursuant to which the **named insured** processes **bank card** transactions on behalf of such entity.

**MID** means a Merchant Identification Number, which is a unique number assigned to a location where a **merchant** accepts **bank cards** for payment.

**Post event services expenses** means reasonable fees and expenses incurred by the **named insured** or a **merchant** with our prior written consent, for any service specifically approved by **us** in writing, including without limitation, identity theft education and assistance and credit file monitoring. Such services must be provided by or on behalf of the **named insured** or a **merchant** within one (1) year following discovery of a **data security event** covered under this **policy** to a **cardholder** whose **cardholder information** is the subject of that **data security event** for the primary purpose of mitigating the effects of such **data security event**.

**Security event expenses** means **card association assessments**, **forensic audit expenses** and **card replacement expenses**

### **COVERAGE SCOPE**

The program provides benefits to **merchants** only if a **data security event** is reported to the contact number stated above as soon as such **merchant** becomes aware of such **data security event**, [but in all events within thirty (30) days of discovery of such **data security event**.] The **merchant** will need to provide details on the **data security event** including, but not limited to: a complete description of the **data security event**; number of **cardholders** affected by the **data security event**; all correspondence from any **card association** regarding the **data security event** and any other pertinent information requested by or on behalf of the Named Insured.

### **EXCLUSIONS**

The **Program** shall not apply to:

1. any fines or assessment levied against the **named insured** or a **merchant** that are not the direct result of a **data security event**;
2. any **data security event** arising out of any software not within the control of the **merchant**; provided, however, this exclusion shall not apply to a **data security event** arising out of a virus, Trojan horse or other software used by a third party to obtain fraudulent access to data on a **merchant's** computer system or to collect data in transit to or from a **merchant's** computer system;
3. any **data security event** arising out of a breach in a computer system in which multiple **merchants**, with no legal relationship to one another, have hosted accounts or share a common database, operating system or software applications;
4. any **data security event** relating to a **participating merchant** which has experienced a prior **data security event** unless such **merchant** was later certified as PCI compliant by a qualified security assessor;
5. any **data security event** arising out of a **merchant** allowing any party (other than its employees or the **named insured**) to hold or access **cardholder information**;
6. any **data security event** involving: (i) a **merchant** categorized by any **card association** as "Level 1" or (ii) a **merchant** that processed more than six million (6,000,000) **bank card** transactions during the twelve month period prior to the **policy period**;
7. any expenses, other than **security event expenses** and **post event services expenses**, incurred by the participating **merchant**, arising out of or resulting, directly or indirectly, from a **data security event**, including without limitation, expenses incurred to bring a **merchant** into compliance with the PCI Data Security Standard or any similar security standard;
8. any **data security event** that was not properly reported to **us** during the **notice period**;
9. any **data security event** occurring before the effective date of the agreement between the relevant **merchant** and the **named insured** to process **bank card** transactions, or after the termination of such agreement;
10. any expenses incurred for, or as a result of, regularly scheduled, recurring or routine security assessments, regulatory examinations, inquiries or compliance activities.

### **PROGRAM LIMIT**

1. The Aggregate Limit of Insurance is the most this policy shall pay for all coverages combined, regardless of the number of data security events, for all **security event expenses** and **post event services expenses** resulting from all **data security events** first discovered by the **named insured** during the **policy period** and reported to us within the **notice period**.
2. All **security event expenses** and **post event services expenses** resulting from the same, continuous, related or repeated **data security event** shall be subject to the terms, conditions, exclusions and Aggregate Limit of Insurance of the policy issued by **us** to the **named insured** in effect at the time the first such **data security event** is first discovered by the

**named insured.**

3. The most we shall pay for the total of all **security event expenses** and **post event services expenses** arising out of or relating to any **merchant** is the Per **Merchant** Sublimit regardless of the number of **data security events** first discovered by the **named insured** during the **policy period** and reported to us within the **notice period**. The Per **Merchant** Sublimit of Insurance is part of, and not in addition to the Aggregate Limit of Insurance.

#### **INSURANCE POLICY**

The **Program** is backed by an insurance policy (the "**Policy**") issued to Named Insured by AIG Specialty Insurance Company ("AIG"), ("us"), or ("our"), a subsidiary of AIG Inc. Although Named Insured may authorize AIG to make payments to, or on behalf of, a **merchant**, and **merchants** are not "insureds" or beneficiaries under the policy.