



PRIVACY AND SECURITY BREACH EXPENSE COVERAGE

Endorsement No.: 8
Policy No.:

Effective Date Of Endorsement:

Issued To:

In consideration of the payment of the premium, it is hereby understood and agreed that, for the purpose of the coverage provided by this endorsement only, the **Insurer** agrees as follows:

I SCHEDULE OF LIMITS AND DEDUCTIBLE

(A) Insuring Agreements Specific Limit of Liability:

(such amounts are part of, and not in addition to, the Endorsement Limit of Liability)

Coverage A:

Privacy Breach Consulting Services Unlimited Aggregate Limit of Liability each **Policy Period**

Coverage B:

Regulatory Research and Compliance Expense Aggregate Limit of Liability each **Policy Period**

Coverage C:

Forensic Investigation Expense Aggregate Limit of Liability each **Policy Period**

Coverage D:

Notification Expense Reimbursement Aggregate Limit of Liability each **Policy Period**

Coverage E:

Notification Recipient Services Aggregate Limit of Liability each **Policy Period**

Endorsement Limit of Liability:

Aggregate Limit of Liability each **Policy Period**
(for Insuring Agreements B, C, D and E combined)

(B) Deductible

(A) Coverage A: \$0.00 each **Privacy Breach**
(B) Coverages B, C, D and E: each **Privacy Breach**

II INSURING AGREEMENTS

The **Insurer** will provide the following services and expense coverages as described below, if the **Insured** has a **Privacy Breach** that is:

- (i) discovered by the **Insured** during the **Policy Period**; and
- (ii) reported to the **Insurer** as soon as possible and no later than 30 days from the **Insured's** discovery of the **Privacy Breach**.

COVERAGE A: PRIVACY BREACH CONSULTING SERVICES

The **Insurer** shall pay on behalf of the **Insured** all **Expenses**, up to the Privacy Breach Consulting Services Limit of Liability stated in Section I, incurred in the provision of the following consulting services by a **Service Provider** for a covered **Privacy Breach**:

- (i) evaluation of **Privacy Breach** situation, assessment of privacy, regulatory and legal impacts and recommendation of best practice approach for notification and remediation;
- (ii) provision of generic notification letter template to provide assistance in drafting an incident specific notification letter;
- (iii) provision of generic FAQ template to be completed by the **Insured** following a **Privacy Breach**; and

- (iv) assistance with media relations when required by applicable **Data Protection Authorities** or due to the size and scope of the **Privacy Breach**.

COVERAGE B: REGULATORY RESEARCH AND COMPLIANCE EXPENSE

The **Insurer** shall pay on behalf of the **Insured** all **Legal Expenses**, up to the Regulatory Research and Compliance Expense Limit of Liability stated in Section I, incurred from a covered **Privacy Breach**, to consult a lawyer to provide the **Insured** with:

- (i) analysis of applicable notification requirements pursuant to provincial and/or federal notification requirements or recommendations of any provincial or federal **Data Protection Authorities**;
- (ii) review and sign off of compliance with applicable provincial and/or federal notification requirements or recommendations of any provincial or federal **Data Protection Authorities**; or
- (iii) an overall process of handling the **Privacy Breach** that complies with applicable provincial and/or federal notification requirements or recommendations of any provincial or federal **Data Protection Authorities**.

COVERAGE C: FORENSIC INVESTIGATION EXPENSE

The **Insurer** shall pay on behalf of the **Insured** all **Forensic Investigation Expenses**, up to the Forensic Investigation Expense Limit of Liability stated in Section I, associated with the necessary technology and / or security forensic investigations of a covered **Privacy Breach**. Coverage shall be available for, and limited to, the investigation into the technology related aspects of the **Privacy Breach** to determine the nature, cause, scope and specific **Data Subjects** impacted by the **Privacy Breach**, including, when necessary, the analysis of:

- (i) networks;
- (ii) servers;
- (iii) terminals;
- (iv) hard drives; and
- (v) other technology.

COVERAGE D: NOTIFICATION EXPENSE REIMBURSEMENT

The **Insurer** shall reimburse the **Insured**, up to the Notification Expense Reimbursement Limit of Liability stated in Section I, for all **Expenses** incurred by the **Insured** following a covered **Privacy Breach** for the preparation, printing, mailing, postage and delivery of notification letters sent by a **Service Provider** to **Notification Recipients** via postal service if:

- (i) the situation dictates notification via hard copy letter;
- (ii) a **Data Protection Authority** requires hard copy letter notification; or
- (iii) hard copy letter notification is the most effective method of notification to affected **Data Subjects**, subject to the **Insurer's** prior written consent.

COVERAGE E: NOTIFICATION RECIPIENT SERVICES

The **Insurer** shall pay on behalf of the **Insured** all **Expenses**, up to the Notification Recipient Services Limit of Liability stated in Section I, incurred in the provision of the following services by a **Service Provider** for a covered **Privacy Breach** to all **Notification Recipients**:

- (i) a toll free telephone number (Crisis Response Line) for **Notification Recipients** to call to address issues, questions or concerns regarding the **Privacy Breach**. This includes the assignment of a live, personal **Fraud Specialist** to provide all necessary services and information on a one on one basis;
- (ii) assistance with ordering free credit reports for evaluation and review of any suspected or actual fraudulent activity; and
- (iii) **Identity Fraud Remediation Services** provided to notification recipients in cases of **Identity Fraud** or **Account Takeover**.

III DEFINITIONS

Whenever appearing in this endorsement, words and phrases appearing in **bold type** shall have the meanings set forth in this Privacy and Security Breach Expense Coverage endorsement. These Definitions apply to the singular and the plural of these terms as circumstances and context require.

Account Takeover means the unauthorized use of a natural person's account as a result of a **Privacy Breach**.

Corporation means the **Parent Corporation** and any **Subsidiary**.

Data means **Private Information** and/or the **Personal Health Information** of a **Data Subject**.

Data Protection Authority means any Canadian federal or provincial government agency responsible for oversight and application of applicable privacy, data protection and privacy breach laws and regulations or similar federal or state government agency of the United States of America.

Data Subject means any natural person who is the subject of **Private Information** and/or **Personal Health Information** collected, stored or processed by the **Insured** in the course of everyday business.

Expenses means all reasonable and necessary costs, charges, fees (but not including legal fees) and expenses incurred, whether paid by the **Insurer** or by the **Insured** with the **Insurer's** prior written consent. **Expenses** does not include loss of earnings or salaries or other compensation paid by the **Insured**.

Forensic Investigation Expenses means all reasonable and necessary costs, charges, fees (but not including legal fees) and expenses incurred, whether paid by the **Insurer** or by the **Insured** with the **Insurer's** prior written consent. **Forensic Investigation Expenses** does not:

- (i) include loss of earnings or salaries or other compensation paid by the **Insured**; or
- (ii) cover the repair or remediation of the underlying cause of the **Privacy Breach**.

Fraud Specialist means an expert retained by the **Insurer** on behalf of the **Insured** to assist **Notification Recipients** in resolving the fraudulent use, or suspected fraudulent use, of **Personal Information** and to restore it to pre-incident status. This assistance may include assistance in contacting credit reporting agencies, credit grantors, collection agencies, and governmental agencies or other activities needed to fully restore the identity of the individual.

Identity Fraud means the actual deceptive use of the **Personal Information** of a natural person (living or dead) in connection with the perpetration of a fraud including, but not limited to, impersonating another and the creation of fraudulent credit accounts.

Identity Fraud Remediation Services means services provided by a **Fraud Specialist** to resolve the fraudulent use, or suspected fraudulent use of **Personal Information** and/or **Personal Health information** and to restore said **Personal Information** and/or **Personal Health information** to pre-incident status.

Insured means the **Corporation**.

Insurer means Trisura Guarantee Insurance Company.

Legal Expenses means all reasonable and necessary costs, charges, fees, and expenses incurred, whether paid by the **Insurer** or by the **Insured** with the **Insurer's** prior written consent, to consult a lawyer. **Legal Expenses** does not:

- (i) include loss of earnings or salaries or other compensation paid by the **Insured**; or
- (ii) cover costs incurred in the defence of the **Insured** against any claim made by a third party.

Malicious Code means a worm, virus, Trojan, BOT or other piece of computer code, software, spyware or malware that is used to illicitly collect, destroy, alter, retrieve or affect computer software and/or **Data** on a computer system, network, storage device, PDA or other peripheral device; and on the date the **Privacy Breach** occurred, is named and recognized by the CERT Coordination Centre, or any industry acceptable third party antivirus, anti-malware or other solution that monitors malicious code activity.

Management Control means:

- (i) owning interests representing more than 50% of the voting, appointment or designation power for the selection of a majority of: the board of directors or equivalent governing body of a corporation; the management committee members of a joint venture or partnership; or the members of the management board of a limited liability company; or
- (ii) having the right, pursuant to written contract or the by-laws, charter, operating agreement or similar documents of the **Corporation**, to elect, appoint or designate a majority of: the board of directors or equivalent governing body of a corporation; the management committee of a joint venture or partnership; or the management board of a limited liability company.

Notification Recipient means a **Data Subject** who is, or is to be, notified by the **Insured** that **Private Information** and/or **Personal Health Information** is exposed or potentially exposed to an unauthorized third party or multiple third parties through a **Privacy Breach** that is experienced by the **Insured** or a third party for whom the **Insured** is responsible, including but not limited to vendors, auditors, and/or other third parties with whom the **Insured** shares **Data** in the course of doing business.

Parent Corporation means the entity named in Item 1 of the Declarations.

Personal Health Information or “**PHI**” means the following definition as provided by the Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5, and with respect to any natural person, whether living or deceased, means:

- (i) information concerning the physical or mental health of the individual;
- (ii) information concerning any health service provided to the individual;
- (iii) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
- (iv) information that is collected in the course of providing health services to the individual; or
- (v) information that is collected incidentally to the provision of health services to the individual.

However, **Personal Health Information** also includes any applicable expansions or refinements of the above definition based on applicable provincial laws and/or regulations.

Policy Period means the period of time from the effective date of this endorsement to the earlier of the expiration date shown in Item 2 of the Declarations or the effective date of cancellation of this Policy.

Privacy Breach means the loss, theft, or accidental release of **Data** involving one or more **Data Subjects**.

Private Information, Personal Information or “**PI**” means any piece of information, which can potentially be used to uniquely identify an individual and could be used to facilitate **Identity Fraud**. This information may include, but is not limited to the following subcategories:

- (i) identification and contact information;
- (ii) government issued identification numbers; or
- (iii) financial information.

Service Provider means a vendor selected by the **Insurer**.

Subsidiary means any entity in which the **Parent Corporation** has or had **Management Control**, either directly or indirectly through one or more other **Subsidiaries**:

- (i) on or before the inception date of this Policy;
- (ii) after the inception date of this Policy by reason of being created or acquired by the **Parent Corporation** after such date, and whose assets do not exceed 25% of the consolidated assets of the **Corporation** as of the inception date of this Policy; or
- (iii) after the inception date of this Policy by reason of being created or acquired by the **Parent Corporation** after such date, and whose assets exceed 25% of the consolidated assets of the **Corporation** as of the inception date of this Policy, but only: (i) for a period of 90 days from the date upon which it became a **Subsidiary**; or (ii) until the end of the **Policy Period**; whichever occurs first (referred to as the Auto-Subsidiary Period).

The **Insurer** shall extend coverage to any **Subsidiary** described in (iii) above beyond its respective Auto-Subsidiary Period if during such Auto-Subsidiary Period:

- (i) written notice of the acquisition or creation of such **Subsidiary** is given to the **Insurer** by the **Parent Corporation**;
- (ii) the **Parent Corporation** provides the **Insurer** with such information in connection therewith as the **Insurer** may deem necessary;
- (iii) the **Parent Corporation** accepts any special terms, conditions, exclusions or additional premium charge as may be required by the **Insurer**; and
- (iv) the **Insurer**, at its sole discretion, agrees to provide such coverage and confirms such agreement in writing.

An entity becomes a **Subsidiary** when the **Parent Corporation** acquires **Management Control** of such **Subsidiary**, either directly or indirectly through one or more other **Subsidiaries**. An entity ceases to be a **Subsidiary** when the **Parent Corporation** ceases to have **Management Control** of such **Subsidiary**, either directly or indirectly through one or more other **Subsidiaries**.

In all events, coverage as is afforded under this endorsement shall only apply to a **Privacy Breach** occurring after the effective date upon which the **Parent Corporation** acquired **Management Control** of such **Subsidiary** and prior to the date upon which the **Parent Corporation** ceased to have **Management Control** of such **Subsidiary**.

IV EXCLUSIONS

The **Insurer** will not provide coverage to the **Insured**:

- (1) for any costs or expenses based upon, arising out of, or attributable to the **Insured's**, or any of the **Insured's** partners, directors, trustees or employees whether acting alone or in collusion with others, intentional involvement in a **Privacy Breach**;
- (2) for a **Privacy Breach** based upon, arising out of, or attributable to any fraudulent, deceptive or criminal activity, error or omission, or any deliberate, reckless or knowing violation of the law by the **Insured**, any of the **Insured's** partners, directors, trustees or employees whether acting alone or in collusion with others, or whether occurring during or outside of the hours of employment;
- (3) for any costs or expenses based upon, arising out of, or attributable to the intentional or reckless disregard for the handling, treatment, transfer and security of **Personal Information** and/or **Personal Health Information** in the **Insured's** possession, control or custody;
- (4) for any costs or expenses to investigate or remedy any deficiency, except as specifically provided under Section II. This includes, but is not limited to, any deficiency in the **Insured's** employee management, vendor management, internal systems, procedures, computer network/system firewall, computer network/system antivirus or physical security that may have contributed to a **Privacy Breach**;
- (5) for any costs or expenses arising out of criminal investigations or proceedings;
- (6) for any costs or expenses based upon, arising out of, or attributable to any **Privacy Breach** that results in the loss of **Data** due to **Malicious Code**, if the failure to detect that code was due to any failure to install or properly implement any:
 - (i) applications;
 - (ii) software;
 - (iii) firewall(s);
 - (iv) anti-virus;
 - (v) anti-spyware;
 - (vi) software or system patches or updates; or
 - (vii) any other reasonable precautions.
- (7) for any charges, penalties, fines or fees imposed by any financial institution, provincial or federal **Data Protection Authorities**, courts of law, or any other entity;
- (8) for any costs or expenses based upon, arising out of, or attributable to the **Insured's** knowledge of any **Privacy Breach** occurring prior to the inception date of this endorsement;
- (9) for any costs or expenses incurred as a result of any third party liability claim and/or for any related defence costs;
- (10) for any costs or expenses based upon, arising out of, or attributable to any threat, extortion or blackmail including, but not limited to, ransom payments and private security assistance;
- (11) for a **Privacy Breach** involving the **PI** or **PHI** of **Data Subjects** who are not Canadian residents with a valid social insurance number or residents of the United States of America with a valid social security number;
- (12) for any costs or expenses based upon, arising out of, or attributable to the **Insured's** failure to cooperate with and provide full disclosure of the circumstances surrounding the **Privacy Breach** to the **Insurer**, applicable federal, provincial, territorial, or state regulators, law enforcement personnel, or any **Service Provider**;
- (13) for any other costs or expenses not provided for under Section II; or

- (14) for any costs or expenses based upon, arising out of, or attributable to liability assumed by the **Insured** under any contract or agreement.

V LIMITS OF LIABILITY

- (A) The Endorsement Aggregate Limit of Liability stated in Section I of this endorsement is the maximum aggregate liability of the **Insurer** with respect to all covered **Privacy Breaches** under Insuring Agreements B, C, D and E discovered in each **Policy Period**.
- (B) The Insuring Agreements Specific Limit of Liability stated in Section I of this endorsement is the maximum aggregate liability of the **Insurer** under each Insuring Agreement with respect to all covered **Privacy Breaches**, which amounts shall be part of, and not in addition to, the Endorsement Aggregate Limit of Liability.

VI DEDUCTIBLE

The deductible indicated in the Section I (B) applies to all coverages under this endorsement. The deductible applies to each **Privacy Breach** reported during the **Policy Period** and shall be borne by the **Insured** uninsured and at its own risk.

VII NOTICE OF CLAIM

- (A) The **Insured** shall, as a condition precedent to its rights under this endorsement, give written notice to the **Insurer** of a **Privacy Breach** within 30 days from the **Insured's** discovery of such **Privacy Breach**.
- (B) Any notice shall be deemed to have been given and received on the day and at the time it is received by the **Insurer** at the following address:

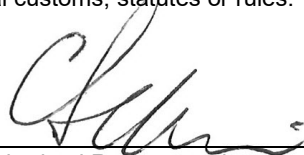
Corporate Risk Claims Department
Trisura Guarantee Insurance Company
333 Bay Street, Suite 1610, Box 22
Toronto, ON M5H 2R2
Fax: (416) 214-9597
Email: claims@trisura.com

VIII GENERAL CONDITIONS

- (A) The **Insured** agrees to use due care to prevent a **Privacy Breach**. This includes, but is not limited to, adherence to industry standards for the protection of **Data** from a **Privacy Breach**.
- (B) The **Insured** agrees to consult with a **Service Provider** and the **Insurer** before issuing any communication to **Notification Recipients**. Any communication or services promised to **Notification Recipients** prior to a consultation will not be covered.
- (C) The **Insured** must cooperate with and provide full disclosure of the circumstances surrounding the **Privacy Breach** to the **Insurer**, applicable federal, provincial, territorial, or state regulators, law enforcement personnel, or **Service Provider**.
- (D) Upon discovery of a **Privacy Breach**, the **Insured** must make reasonable efforts to secure and protect the remaining **Data** still in the **Insured's** control.
- (E) The **Insurer** will pay for services associated with Section II only if they are provided through a **Service Provider**. Approval for an alternate **Service Provider** must be obtained prior to the consultation process. The **Insurer** will only pay reasonable and customary charges associated with services covered under this endorsement provided by the alternate **Service Provider**.
- (F) The **Insurer** cannot, and does not, guarantee that after the **Service Provider** has provided the applicable services the problems associated with the covered **Privacy Breach** will be eliminated.

(G) Services provided by the **Service Provider** to **Notification Recipients** may vary based on individual circumstances and location due to adherence to local customs, statutes or rules.

All other terms and conditions remain unchanged.



Authorized Representative

SPECIMEN