PREMIER canada

Form #GRCYB300 - Group Employee Benefit - Cyber Policy (Claims Made and Reported)

(Rev. 1 January 2024)

This **Policy** is intended to provide the protection that has been requested by **you**. As a legal contract between the **Underwriters** and **you** it is important that this **Policy** document is checked to ensure that all the details stated in any Quotation issued prior to the production of this document and the **Declarations Page** (which is attached and forms an integral part of this **Policy**) are correct, and that it reflects **your** understanding of the cover, meets its requirements and is adequate for its needs. If any aspect is unclear, **you** should discuss this **Policy** with its broker.

You or **your** broker must notify the **Underwriters** as soon as is reasonably practicable if there is a discrepancy, omission, if **your** insurance requirements change or of any significant changes which may affect the insurance provided by this **Policy**.

In the Event of an Incident

As soon as the **employee** discovers or suspects that they have been the victim of **a cyber-attack, cyber extortion threat**, or **identity theft**, please call CyberClan. **The employee's** call will be dealt with by a team of specialists who will provide **the employee** with personal assistance throughout the resolution process.

There is no cost to **the employee** beyond **the employee's** standard charge of calling the CyberClan helpline. The **employee** will only incur costs from calling the helpline if there are further actions to be taken as a result of the **cyber-attack, cyber extortion threat, identity theft, credit card fraud of phishing attempt**. Such costs are recoverable under this policy, subject to the terms and conditions of this policy, including the Limit of Liability and Deductible stated in the Declarations page.

CyberClan 24/7 Breach Response Hotline 1-800-673-8651
Email: cyberclaims@cyberclan.com

Understanding this Policy

Coverage under this **Policy** is provided on a claims made and reported basis and applies only to losses discovered by **the employee** during the Period of Insurance and reported to the Underwriters during the Period of Insurance.

This **Policy** must be read in its entirety as Conditions, Exclusions and other limitations apply. The **Insured** must comply with the terms of this **Policy**. Failure to do so may result in refusal or reduction of a claim where that claim has been affected by any failure to comply.

This **Policy** contains different types of insurance coverage. This **Policy** only affords coverage under those insured coverages below that are indicated as purchased in the Declarations Page and as limited therein.

The descriptions in the headings and subheadings of this **Policy** are solely for convenience and reference and are not intended to limit or extend the scope of the provisions.

Terms that appear in bold face type are defined in the Definitions section of this **Policy**. Terms with capitalised first letters are defined in more detail in this

Policy or as the context requires. Please read this **Policy** carefully. Any obligation or payment owed by **Underwriters** shall in every case be subject to the **Limits of Liability** specified in the Declarations Page.

The Deductible applies to each and every cyber extortion threat, cyber-attack, identity theft, credit card fraud, or phishing attempt and if the costs incurred by **the employee** are less than, or equal to the deductible, **we** will not pay for these costs. If the costs incurred from the cyber-attack, cyber extortion threat, identity theft, credit card fraud, or phishing attempt exceed the deductible then **we** will subtract the deductible from this amount and pay the remaining amount up to the Policy Aggregate Limit.

Section I - Insuring Agreements

Section 1.A Cyber Attack

We will pay the reasonable and necessary costs that **the employee** incurs as a direct result of a **cyber-attack** carried out by a **hacker** to:

1. Replace **the employee's computer system**;
2. Restore **the employee's computer system** to the level of functionality that existed prior to the **cyber-attack** occurring. Where it is determined that it is not possible to restore **the employee's computer system** to the level of functionality that existed prior to the **cyber-attack** occurring, **we** will only pay for the costs incurred up to the date of such determination;
3. Retrieve and restore **the employee's data** to **the employee's computer system**; and/or
4. Retrieve and restore **the employee's** personal digital music, digital photographs and digital video that have been downloaded to **the employee's computer system.**

We will not pay for:

1. Any amounts **the employee** paid, or has agreed to pay, as part of any **computer system** maintenance contract;
2. Costs to upgrade or increase the speed, capacity, or functionality of **the employee's computer system** beyond the level that existed prior to the **cyber-attack** occurring; or
3. Costs to re-purchase software, software licenses, programs, digital photographs, music or videos; or
4. Costs that exceed the value of an equivalent **computer system**.

Section 1.B Ransomware

We will pay reasonable and necessary **cyber extortion expenses** and **ransom monies** that **the employee** incurs as a direct result of a **cyber extortion threat.**

We will not pay any **cyber extortion expenses** or **ransom monies** unless **the employee**:

1. Has consulted **our** expert service provider CyberClan in advance to assess the situation;
2. Has made reasonable efforts to determine that the **cyber extortion threat** is credible and genuine; and
3. Has obtained **our** prior written consent before any **ransom monies** are paid.

We will not pay any **ransom monies** if doing so would breach any law or regulation, or any instruction from any law enforcement agency or regulator.

Section 1.C Identity Theft

We will pay the **identity theft expenses** that **the employee** incurs solely and directly because of an actual or suspected **identity theft**.
The employee must inform **our** expert service provider CyberClan as soon as reasonably possible once **the employee** believes **the employee** is a victim of **identity theft.**

Section 1.D Cyber Crime

We will pay for the costs of the charges **the employee** has incurred, the funds **the employee** has transferred or the reasonable and necessary costs of replacing **the employee's** personal documents that **the employee** incurs solely and directly because of **credit card fraud** or **phishing** against **the employee**. All Cyber Crime loss claims must be evaluated by CyberClan to determine whether **the employee** or a third party is accountable for the loss.

We will not cover Cyber Crime:
1. If it is reimbursable by **the employee's** credit card company, bank or other financial institution;
2. From the unauthorized criminal use of **the employee's** credit or debit card by a member of **the employee's** family unless **the employee** is willing to file a police report and/or press charges against the member of **the employee's** family; or
3. For losses arising outside of **the employee's** personal capacity.

Section 1.E Smart Devices and Wearables

If **the employee** discovers that **the employee's connected home device** has become damaged, altered or corrupted as a result of a **cyber-attack** by a **hacker, we** will pay for the cost of restoring this back to its condition prior to the **cyber-attack**.
We will not cover any Smart Devices and Wearables attack where **the employee** has failed to change the default/original password on **the employee's connected home device**.

Section II – Definitions

1. **Computer System** means computer hardware and peripherals networks, including any laptop, mobile phone or tablet, owned by the employee and used solely by the employee for personal purposes and which is located at the employee's home.

2. **Connected home device** means an electronic device or appliance owned by the employee that can send and receive data and is connected to the internet, including but not limited to the employee's laptop, mobile telephone, television, refrigerator, smart speakers or smart watch.

3. **Credit card fraud** means the financial loss as a result of a fraudulent input, modification of data in the employee's computer system that results in money being transferred from the employee's account or a credit arrangement being made.

4. **Cyber-Attack** means unauthorised access to the employee's computer system or the malicious introduction of software designed to disrupt or cause damage to the employee's computer system.

5. **Cyber extortion threat** means a credible threat alongside a demand for ransom monies, which is directed at the employee to:
   a. Release, destroy, disseminate or permanently encrypt data stored in the employee's connected home device or computer system;
   b. Introduce a virus into the employee's connected home device;
   c. Corrupt, damage, disable, destroy, or alter the employee's connected home device, or
   d. Deny, restrict or hinder access to the employee's connected home device or computer system.

6. **Cyber extortion expenses** means costs incurred directly as a result of a **cyber extortion threat** that are not **ransom monies**.

7. **Data** means information held electronically or digitally including code held by **the employee** on **the employee's computer system. Data** does not include software or programs.

8. **Employee** mean current employees of the Insured in the Declarations Page, and any other immediate member of their family aged over 18 and permanently living in the **home.**

9. **Hacker** means anyone except:
   a. The employee
   b. The employee's spouse or partner
   c. A member of the employee's family
   d. A person who resides at the employee's home
   Who targets the employee in order to gain unauthorized access to the employee's computer system.

10. **Home** *means the address of the property used as the employee's primary domestic residence including any outbuildings or garages used for domestic purposes.*

11. **Identity theft** means a fraud committed or attempted using the employee's identifying information without the employee's consent. Such fraud need not be for financial, criminal or other gain. Identity theft does not include cost incurred to a business that is associated with the employee as a result of the identity theft.

12. **Identity theft expenses means the following services provided by CyberClan to restore the employee's identity:**

    a. Access to a toll-free 24/7/365 telephone helpline number for **the employee** to ask questions and address issues or concerns regarding an **identity theft**;

    b. The services of a personal fraud specialist who will assist **the employee** with the following if there is a suspected **identity theft**:
       i. Obtaining a copy of **the employee's** credit report;
       ii. Reviewing **the employee's** credit reports for possible fraudulent activity;
       iii. Placing a fraud alert;
       iv. Facilitating placement of a security freeze; or

v. Other personal fraud assistance upon approval by **us**;

c. The following services for **the employee**, if **the employee** is the victim of an actual **identity theft**:
   i. Creating fraud victim affidavits;
   ii. Assisting in making any phone calls and preparing all documents needed for credit grantor notification and fraud information removal purposes;
   iii. Assisting in the filing of a crime report
   iv. Creating comprehensive case files for insurance and police;
   v. Notifying any relevant government and private agencies; and
   vi. Other identity theft remediation services when warranted and upon prior approval by **us**.

d. Upon request, enrollment in one (1) year of the following services for **the employee**, if **the employee** is an actual victim of **identity theft**:
   i. Single bureau credit monitoring including electronic credit reports and electronic alerts;
   ii. A social security trace which monitors state public records, including court proceedings, bankruptcies, and liens, and which provides electronic notification to the employee;
   iii. Cyber monitoring providing electronic notification of online criminal or fraudulent activity involving the employee's personally identifiable information; or
   iv. Other monitoring services upon prior approval by us.

The above services and associated costs provided by CyberClan are part of and not in addition to the Limit of Liability.

12. **Limit of Liability** means the maximum that **we** will pay in total for the Period of Insurance. The **Limit of Liability** is shown in the Declarations Page.

13. **Phishing** means fraudulent electronic communications purporting to be from a reputable company to induce **the employee** into the transfer of **the employee's** money or personal information including but not limited to passwords or credit card numbers.

14. **Ransom monies** means cash and/or marketable goods to be surrendered by **the employee** or by an authorised third party on **the employee's** behalf to terminate a **cyber extortion threat.**

15. **We/us/our** means the insurer named in the Declarations Page**.**

16. **You/your** means the person named as the Insured in the Declarations Page, and current employees of as the Insured, and any other immediate member of their family over 18 years of age and permanently living in the **home.**

Section III - General Conditions

1. The **cyber-attack, cyber extortion threat, identity theft, credit card fraud**, **phishing** attempt or cyber-crime must be first discovered by **the employee** during the Period of Insurance.

2. **The employee** must report the **cyber-attack, cyber extortion threat, identity theft, credit card fraud or phishing** attempt to **us** no later than fifteen (15) days after the **cyber-attack, cyber extortion threat, credit card fraud** or **phishing** attempt is first discovered by **the employee**.

3. **The employee** must back up original **data** of **the employee's computer system** at least every 30 days. If a service provider processes or stores data for **the employee**, **the employee** must make sure that the terms of the contract between **the employee** and the service provider allow **data** to be backed up.

4. **The employee** must change the passwords on **the employee's computer system** or **connected home device** from the default password that existed on the **computer system** or **connected home device**.

5. **The employee** must have anti-virus software installed on **the employee's computer system.**

6. If there is any other insurance covering **the employee's** claim, **we** will only pay **our** proportionate share of **the employee's** claim.

Section IV – Exclusions

We do not cover:

1. **Bodily Injury**
Physical injury, sickness, disease, or death sustained by any individual and, where resulting from such physical injury only, mental anguish, mental injury, shock or emotional distress;

2. **Physical Perils**
Any loss arising from fire; explosion; implosion; smoke; electrostatic build-up or static electricity; electrical or mechanical failures including spike, brownout or blackout; aircraft impact; vehicle impact; or water damage;

3. **Business Capacity**
Any loss that relates to, or is used for the purposes of, **the employee's** trade, business or profession or any other capacity other than **the employee's** own personal capacity;

4. **Confiscation by Public Authority**
Any loss arising from the seizure, confiscation, nationalization, requisition or destruction of **the employee's computer system**, **connected home device**, or any other **data**, electronic equipment or any other property by or under order of any government or public authority;

5. **Connected Device Liability**
Any liability arising from **the employee's connected home device.**

6. **Deficiency or Improvements**
The cost of correcting any failings in procedures, systems or security or the cost of any normal **computer system** maintenance;

7. **Face to Face Ransom**
Any **ransom monies** surrendered in a face-to-face encounter;

8. **False Claims**
Any loss arising from a false report of an insured event made by **the employee**, whether acting alone or in collusion with a third party;

9. **Infrastructure Services**
Any loss arising from satellite failure, electrical or mechanical failures including blackout, failures of overhead or subterranean transmission and distribution lines or outage to utility infrastructure, including gas, water and electricity or outage to telecommunications infrastructure including telephone, internet, cable or cloud computing services.

10. **Known Prior Matters**
Any loss arising from any matter that **the employee** was aware of or reasonably ought to have been aware of prior to the inception of this policy;

11. **Legal Liability, Fines or Penalties**
Any amounts owed by **the employee** to a third party for damages, fines or penalties;

12. **Legal Proceedings**
Any costs incurred by **the employee** to institute or defend against legal proceedings against a person or organization;

13. **Loss of Internet connection**
Any loss or costs incurred by the employee as a result of a total, partial, temporary or intermittent outage of internet connection;

14. **Malicious or Criminal Acts**
Any loss arising from willful, intentional, malicious or criminal acts committed by **the employee** or in collusion with a third party;

15. **Natural Perils**
Any loss arising from lightning, wind, windstorm, tornado, cyclone, hurricane, flood, storm surge, sinkhole collapse, earthquake, volcanic eruption, wave, tidal wave, landslide, hail, snow, geomagnetic storm or any other natural physical event however caused;

16. **Property Damage**
Any loss arising from physical injury to, or, destruction of, any tangible property, including any **computer system,** personal property, **connected home device(s)** in the care, custody or control of **the employee** at **the employee's home. Data** is not tangible property;

17. **Theft**
The theft of any of **the employee's** possessions including **the employee's computer system** or **connected home device. We** do not cover **Credit Card Fraud** where **the employee's** credit card has been physically stolen.

18. **Sanctions**
Any claim to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose **us** to any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of the European Union, United Kingdom, Jamaica or United States of America.

19. **Social Media**
The loss or liability arising from the use, whether authorised or not, of any email, social media posting or website;

20. **War or Uprising**
Any loss arising from confiscation, nationalization, requisition, strikes or similar labor actions; war, invasion, or warlike operations, civil war, terrorism, mutiny, rebellion, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military coup or usurped power;