Privacy Breach Expense Coverage and Cyber Event Recovery and Cyber Event Liability Coverage (including Consulting Services) - Form 53000

This endorsement changes the policy. Read the entire endorsement carefully to determine rights, duties and what is and is not covered. Throughout this endorsement, "you" and "your" refer to the Named Policyholder as defined within the insurance policy Declarations Page. The words "we", "us" and "our", refer to the Company providing the insurance. Other words and phrases that appear in "quotation marks" have special meaning and are clarified within the **Definitions**.

Section I – First Party Coverage

Privacy Breach Expense Coverage

"We" will provide the following **Privacy Breach Expense Coverage** through CyberScout or by a vendor approved by "us", as described below if "you" have a "privacy breach" that is:

a. Discovered by "you" during the policy period reflected within the insurance policy Declarations Page;
b. Occurring up to 90 days prior to the policy effective date, but discovered by "you" during the policy period reflected within the insurance policy Declarations Page; and
c. Reported to "us" as soon as possible and within 30 days of "your" discovery of the "privacy breach".

1. **Privacy Breach Pre-Notification Consulting Services:** In the event of a covered "privacy breach", "we" will provide the following consulting services by CYBERSCOUT, or by a vendor approved by "us":

   a. Evaluation of a "privacy breach" situation, assessment of privacy impacts and recommendation of a best practice approach for response notification and remediation;
   b. Provision of a generic notification letter sample template to provide assistance in drafting an incident specific notification letter;
   c. Provision of a generic sample Frequently Asked Questions (FAQ) template to be completed by "you" following a "privacy breach" which enables "fraud specialists" to better inform "notification recipients" of relevant facts. This can be utilized for specifically tailored and/or customized talking points;
   d. Assistance with interaction with regulators and media relations, if and when warranted.

   All of the above are subject to final review and approval by "your" legal counsel.

2. **Notification Expense Reimbursement**: "We" will provide "you" with **Notification Expense Reimbursement** coverage for eligible expenses following a "privacy breach" for services provided by CYBERSCOUT, or by a vendor approved by "us", for costs associated with:
   a. Preparation, printing, mailing, postage and delivery of notification letters sent to "notification recipients" following a "privacy breach"; and
   b. "Notification Recipient Services"

   The above is pursuant to applicable Provincial and/or Federal notification requirements. If there is any other insurance that would apply in absence or in addition to this policy, the insurance under this policy shall only apply as excess insurance over such other insurance.

3. **Monitoring Expense Reimbursement**: On recommendation from "our" counsel, or "us", "we" will provide "you" with coverage for the cost of "monitoring services" for "notification recipients" when warranted. "Monitoring services" will be provided by CyberScout or by a vendor approved by "us". If there is any other insurance that would apply in the absence of or in addition to this policy, the insurance under this policy shall only apply as excess insurance over such other insurance.

4. **Forensic Investigation Expense**: "We" will provide "you" with coverage for costs associated with the necessary technology and/or security forensic investigations of a covered "privacy breach", subject to the **Forensic Investigation Expense** sublimit as shown on the insurance policy Declarations Page. Coverage shall be available for 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:
   a. Networks;
   b. Servers;
   c. Terminals;

d. Hard drives;
e. Other technology.

Forensic Investigation Expenses do not cover the repair or remediation of the underlying problems that caused the "privacy breach."

5. **Legal and Regulatory Research Expense**: "We" will provide "you" with coverage for costs incurred from a covered "privacy breach", to consult a licensed attorney to provide "you" with the following:
   a. Analysis of applicable notification requirements pursuant to Provincial and/or Federal laws and regulations;
   b. Review and sign off on compliance with applicable Provincial and/or Federal notification requirements; and/or
   c. The overall process of handling the "privacy breach" to ensure it complies with applicable Provincial and/or Federal regulations.

Cyber Event Recovery

"We" will provide the following **Cyber Event Recovery** coverage through CyberScout or by a vendor approved by "us", as described below if "you" have an "Cyber Event" that is:

a. Discovered by "you" during the policy period reflected within the insurance policy Declarations Page; and,
b. Occurring up to 90 days prior to the policy effective date, but discovered by "you" during the policy period reflected within the insurance policy Declarations Page; and
c. Reported to "us" as soon as possible and within 30 days of "your" discovery of the "Cyber Event".

1. **Data Restoration**: "We" will pay "your" reasonable and necessary fees and expenses of a professional firm to restore electronic "data" that has been altered, corrupted, or stolen as the result of a "Cyber Event."

2. **Data Ransom, Extortion and Blackmail: "**We" will pay "your" reasonable and necessary fees and expenses of independent forensic analysts, private investigators, or negotiators engaged by "you" and approved by "us" in the event "you" receive a threat of data ransom, extortion, or blackmail resulting from a "Cyber Event." This includes coverage for the payment of the ransom, extortion, or blackmail demand resulting from a "Cyber Event" subject to the **Data Ransom, Extortion and Blackmail** sublimit shown on the insurance policy Declarations Page.

3. **System Restoration: "**We" will pay "your" reasonable and necessary fees and expenses of a professional firm to restore computer programs and/or network operating systems that have been altered, corrupted, or stolen as the result of a "Cyber Event."

4. **Business Interruption:** "We" will pay "your" actual loss of "business income" and reasonable "extra expenses" during the "restoration period" following a "cyber event" up to, but not more than 20% of the **Cyber Event Recovery** limit indicated within the insurance policy Declarations Page. This coverage is subject to a waiting period of 24 hours from the time the "Cyber Event" is discovered by "you".

Section II – Third Party Coverage

Cyber Event Liability

"We" will provide "you" with **Cyber Event Liability** for the services as described below up to the limits shown in the insurance policy Declarations Page for a "Cyber Event" "legal claim", so long as:

a. Notice is provided to "you" during the policy period of this endorsement;
b. "You" report the "legal claim' to "us" within 30 days of receiving the notice; and,
c. Such claim is made against a covered "Cyber Event" which occurred during the policy period and one which "you" provided "Cyber Event" "notification recipient services" through CYBERSCOUT or a vendor approved by "us"; OR
d. Such claim is made against a covered "Cyber Event" which occurred up to 90 days prior to the policy effective date and one which "you" provided "Cyber Event" "notification recipient services" through CYBERSCOUT or a vendor approved by "us".

1. **Cyber Event Defence**: "We" will pay the approved legal "defence costs" resulting from a "legal claim" for a covered "Cyber Event".

2. **"Cyber Event Liability Payment": "**We" will pay the "legal claim" for a covered "Cyber Event" which "you" become legally responsible to pay.

3. **Regulatory Fines and Penalties: "**We" will pay for "fines and penalties" that "you" become legally responsible to pay resulting from a "regulatory proceeding" for a covered "privacy breach" subject to the **Regulatory Fines and Penalties** sublimit shown on the insurance policy Declarations Page.

Limits

The **Privacy Breach Expense Coverage, Cyber Event Recovery** and **Cyber Event Liability Coverage** limits indicated in the insurance policy Declarations Page are the most "we" will pay for a covered "Cyber Event" as specified for the aggregate limit and those expenses which are reflected as sub-limits. Unless specified otherwise, the sub-limits reflected within the insurance policy Declarations Page are included in and not separate from the aggregate limit.

Deductible

The **Privacy Breach Expense Coverage, Cyber Event Recovery** and **Cyber Event Liability Coverage** deductibles indicated within the insurance policy Declarations Page applies to coverage limits specified within **Section I: Privacy Breach Expense Coverage and Cyber Event Recovery** limits and **Section II: Cyber Event Liability Coverage** limits. The Privacy Breach Expense and Cyber Event Recovery deductible applies to each "privacy breach" and/or "cyber event" reported during the policy period. The **Cyber Event Liability** deductible applies to each "legal claim" first made against "you" during the policy period for a covered "cyber event".

Exclusions

"We" will not provide coverage under **Section I: Privacy Breach Expense Coverage** or **Cyber Event Recovery** or for a "legal claim" under **Section II: Cyber Event Liability** based on the following:

1. "Your" intentional involvement in a "Privacy Breach, "Cyber Event", or "Cyber Event" "legal claim".
2. A "privacy breach" resulting from any fraudulent, deceptive or criminal activity, error or omission, or any deliberate, reckless or knowing violation of the law by "you", any of "your" partners, directors, trustees whether acting alone or in collusion with others; or whether occurring during or outside of the hours of employment;
3. A "privacy breach" of "data" does not include the fraudulent use of a business name, business entity, business association or any action identifying a business.
4. Intentional or reckless disregard for the handling, treatment, transfer and security of "personal information" in "your" possession, control or custody
5. Expenses to investigate or remedy any deficiency, except as specifically provided under **Section I: Privacy Breach Expense Coverage**. This includes, but is not limited to, any deficiency in "your" 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".
6. Any "defence costs" or fines resulting from criminal investigations or proceedings.
7. Known "privacy breaches", occurring prior to the policy coverage period of this endorsement or unknown "privacy breaches" occurring more than 90 days prior to the policy period.
8. Costs incurred via third party liability and/or "defence costs".
9. Any threat, extortion or blackmail including but not limited to, ransom payments and private security assistance not caused by a "Cyber Event."
10. A "Privacy Breach" or "legal claim" for a "Cyber Event" involving the "personal information" of "data subjects" who are not residents of North America with a valid Social Security Number or Social Insurance Number.
11. "Your" failure to cooperate with and provide full disclosure of the circumstances surrounding the "Privacy Breach" or "Cyber Event" to "us", and any applicable Provincial and/or Federal regulators, law enforcement personnel, CYBERSCOUT, and/or other designated service providers.
12. Any other expenses not provided for under the **Section I: Privacy Breach Expense Coverage**.
13. Legal obligations arising by reason of assumption of liability in a contract or agreement.
14. "Cyber Events" covered by another policy.
15. Cost to research or correct any deficiency.

16. Loss of the internet, an internet service provider, any computer or computer system not owned or leased to “you” and operated under “your” control.
17. Subsequent “legal claims” resulting from a “Cyber Event” that are covered by another policy;
18. Any type of bodily injury or property damage.
19. Resulting from “your” financial insolvency or bankruptcy.
20. Prior to the policy period coverage of this endorsement, “your” knowledge of deficiencies in “your” computer systems or security processes.
21. Resulting from a “legal claim” made against “you” for prior known “Cyber Events”, occurring prior to the policy period coverage of this endorsement; or unknown “Cyber Events” occurring more than 90 days prior to the policy period.
22. Resulting from a “legal claim” made against “you” by a subsidiary or entity owned whole or in part by “you”.
23. “Legal claim” expenses associated with satisfying a non-monetary judgment made against “you”.
24. Any threat, extortion or blackmail including but not limited to, ransom payments and private security assistance that would not otherwise be covered under **Cyber Event Recovery, Data Ransom, Extortion and Blackmail**.
25. A “legal claim” made against “you” based on any discrimination including race, creed, religion, age, handicap, sex, marital status, or financial condition.
26. “Malicious Code” in connection with hardware or software created, produced, or modified by “you” for sale, lease, or license to third parties.

Conditions

1. “You” agree to use due care to prevent a “Cyber Event”. This includes, but is not limited to, adherence to industry, privacy, legal, and regulatory standards for the protection of “data” from a “Cyber Event” as defined by this endorsement.
2. Before issuing any communication to “notification recipients”, “you” agree to consult with CYBERSCOUT and “us”. Any communication or services promised to “notification recipients” prior to a consultation will not be covered.
3. “You” must cooperate with and provide full disclosure of the circumstances surrounding the “Cyber Event” to “us” and applicable Provincial and/or Federal regulators, law enforcement personnel, CYBERSCOUT, and/or other designated service providers.
4. Upon discovery of a “privacy breach” and/or a “cyber event”, “you” must make reasonable efforts to secure and protect the remaining “data” still in “your” control.
5. “We” will pay for services associated with **Section I: Privacy Breach Expense Coverage** only if they are provided through CYBERSCOUT or a vendor approved by “us”. Approval for an alternate vendor must be obtained prior to the consultation process. “We” will only pay reasonable and customary charges associated with services covered under this endorsement provided by the alternate vendor.
6. “We” cannot guarantee after CYBERSCOUT, or a vendor approved by “us”, has provided the applicable services, that the problems associated with the covered “privacy breach” will be eliminated.
7. Services provided to “notification recipients” by CYBERSCOUT, or a vendor approved by “us”, may vary based on individual circumstances and location (due to adherence of local customs/statutes/rules.)
8. “You” must make reasonable efforts to secure and protect the remaining “data” still in “your” control.
9. “You” agree not to make any payment or incur any expenses regarding **Section II: Cyber Event Liability, Regulatory Fines and Penalties** without “our” prior written consent, unless “you” are doing so at “your” own expense.
10. “We” have the right and duty to select counsel to defend “you” against a “legal claim” under **Section II: Cyber Event Liability, Regulatory Fines and Penalties**. However, “we” are not obligated to defend “you” against a “legal claim” in which this coverage does not apply.
11. With “your” written consent, “we” may settle a “legal claim” in any way “we” consider reasonable. If “you” withhold consent, then “our” liability for damages is limited to what “we” would have paid as of the date of the proposed settlement. “You” assume any further responsibilities and expenses regarding settlement of the “legal claim”.

Definitions

1. **“Account Takeover”**: The unauthorized use of a person’s existing financial account(s) or services.
2. “**Business Income”:** During the “restoration period,” the net income (net profit or loss before income taxes) that would have been earned or incurred and/or the continuing and normal operating expenses incurred, including payroll.

3. **"Cyber Event"**: An event caused by a "privacy breach" or "network security failure."
4. **"Cyber Event Liability Payment":** The amount included within a "legal claim" for a covered "Cyber Event" which "you" become legally responsible to pay.
5. **"Data"**: May be interchangeable with the term Information and includes "Personal Information" and/or other information of a "data subject" that is reasonably deemed as sensitive, unpublished information.
6. **"Data Subject":** An individual human being whose "Personal Information (PI)" is lost, stolen, improperly accessed, accidentally released or accidentally published due to a "privacy breach".
7. **"Defence Costs"**: The reasonable and necessary expenses incurred to investigate, settle, or defend a "legal claim" for a covered "Cyber Event".
8. "**Denial of Service":** An interruption in an authorized user's access to a computer network, typically one caused with malicious intent.
9. "**Extra Expense":** Reasonable and necessary expenses "you" incur to operate the business during "restoration period" over and above the normal costs "you" would have incurred to operate the business during the same period had no "Cyber Event" occurred.
10. **"Fines and Penalties"**: Any monetary penalty or civil fine imposed in a regulatory proceeding as punishment for "your" actual or alleged violation of a "privacy law". This definition does not include any awards for harm or to reimburse another's expense.
11. **"Fraud Alert**": A warning that is placed on the "notification recipient's" credit bureau report signaling to potential creditors that the "notification recipient" may be or is at risk of being a victim of "identity fraud".
12. **"Fraud Specialist":** An expert retained by CYBERSCOUT or a vendor approved by "us" to assist "notification recipients" in responding to questions on the "privacy breach" notification communication, resolving the fraudulent use, or suspected fraudulent use, of "personal information" and to restore identity 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.
13. **"Identity fraud":** The actual deceptive use of the "personal information" of another person (living or dead) in connection with various frauds, including but not limited to impersonating another and the creation of credit accounts.
14. **"Legal claim"**: A written notice or demand for monetary or non-monetary relief for a covered "Cyber Event". This includes even if the assertions are false or fraudulent.
15. **"Malicious Code"**: Any loss of "data" or unauthorized access to "data" that results from a worm, virus, Trojan, bot, or other piece of computer code, software, spyware or malware that is used to 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 Cyber Event occurred is named and recognized by the CERT Coordination Center, or any industry acceptable third party antivirus, anti-malware or other solution that monitors "malicious code" activity.
16. **"Monitoring Services":** For "notification recipients" who are victims of "identity fraud" or, if in the event a proactive approach to watch and identify potential identity misuse is offered, a service that monitors various "data" sets of a "data subject" that may indicate fraud. Examples of services may include:
    a. Enrollment in one year of credit monitoring with alerts. Includes 2-in-1 credit report. Monitors changes in enrolled "notification recipient's" credit file to identify fraudulent activity and measures the progress of resolution; and/or
    b. Enrollment in one year of fraud monitoring providing electronic notification to enrolled "notification recipient" of changes in personal identifiers (i.e. Social Insurance Number, Department of Motor Vehicle, address, etc.), in more than 1000 monitored databases. Identifies additional fraud and measures the progress of resolution; and/or
    c. For "privacy breaches" necessitating provision of "monitoring services", an Internet based enrollment platform in addition to phone-in enrollment options will be offered.
17. **"Network Security Failure":** Failure of "your" network security permitting unauthorized access to "data", computer systems, or electronic hardware owned by "you", intrusion of "malicious code" to "your" computer systems or electronic hardware owned by "you", forwarding or propagating "malicious code" to third parties, and/or "denial of service" preventing access to "data" for which a party is entitled.
18. **"Notification Recipient":** A "data subject" who is notified by "you" that "Personal Information" is exposed or potentially exposed to an unauthorized third party or multiple third parties through a "data breach" that is committed by "you" or a third party for whom "you" are responsible, including, but not limited to vendors, auditors, and/or other third parties with whom "you" share "data" in the course of doing business.

19. **"Notification Recipient Services"**: "We" will provide the following services for a covered "data breach" to "notification recipients" when such notice is required by law or as best practice:
    a. "Identity fraud" Remediation Services provided to "notification recipients" in cases of "identity fraud" or "account takeover";
    b. A toll-free telephone number (Data Breach Response Line) for "notification recipients" to call to address issues, questions or concerns regarding the "data breach". This includes the assignment of a live, U.S. based personal "fraud specialist" to provide approved and necessary services and information on a one-on-one basis;
    c. Assistance to "notification recipients" in placing a "fraud alert" for those who believe they are at risk of becoming or have become "identity fraud" victims.
20. **"Personal Information":** means any piece of information (including personal health information as defined under applicable law), 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:
    a. Identification and contact information;
    b. Government issued identification numbers;
    c. Financial information.
21. "**Privacy Breach": T**he loss, theft, accidental release, accidental publication of "data" involving one or more "data subjects". Includes loss or unauthorized access to "data" involving one or more "data subjects" resulting from "malicious code." Synonymous terms used for "privacy breach" may include the following: "Personal Information" Security Breach, "Data" Compromise, Database Breach, Information Compromise, Enterprise Security and Information Breach.
22. **"Privacy Law"**: An act, regulation, statute, framework, guidance or law that requires the protection of a "data subject's" "personal information" by "you".
23. **"Regulatory Proceeding":** A non-criminal proceeding that is brought as the result of an actual or alleged violation of a "privacy law" by a regulatory agency.
24. **"Restoration Period":** The time period, after the first 24 hours immediately following the time the "Cyber Event" is discovered by you and continues until the date all "**data restoration**" and/or "**system restoration**" directly related to the "Cyber Event" has been completed or could have been completed with proper due care and diligence.
25. **"We", "Us"** and "**Our":** The words "we", "us" and "our" refer to the Company providing the insurance.
26. **"You"** and "**Your":** Throughout this endorsement, "you" and "your" refers to the Named Policyholder as defined with the insurance policy Declarations Page.