Privacy Breach Expense Coverage (including Consulting Services) - Form 52000

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 sublimit as shown on the insurance policy Declarations Page. Coverage shall be available for 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:

   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" complies with applicable Provincial and/or Federal regulations.

Limits

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

Deductible

The **Privacy Breach Expense Coverage** deductible indicated within the insurance policy Declarations Page applies to all coverages for which a deductible is shown under this section. The deductible applies to each "privacy breach" reported during the policy period.

Exclusions

"We" will not provide coverage under **Section I: Privacy Breach Expense Coverage** based on the following:

1. "Your" intentional involvement in a "privacy breach";
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 of the handling, treatment, transfer and security of "personal information" in "your" possession, control or custody;
5. Expense 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. Expenses arising out of criminal investigations or proceedings;
7. Charges, penalties, fines or fees of affected financial institutions, Provincial or Federal Privacy Regulators, courts of law, and any other entity;
8. 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;
9. Costs incurred via third party liability and/or defense costs;
10. Any threat, extortion or blackmail including but not limited to, ransom payments and private security assistance;
11. A "privacy breach" involving the "Personal Information" of "data subjects" who are not residents of North America with a valid Social Security Number or Social Insurance Number;
12. "Your" failure to cooperate with and provide full disclosure of the circumstances surrounding the "privacy breach" to "us", applicable Provincial or Federal regulators, law enforcement personnel, CYBERSCOUT and/or other designated service providers;
13. Any other expenses not provided for under the **Section I: Privacy Breach Expense Coverage**;
14. Legal obligations arising by reason of assumption of liability in a contract or agreement.

Conditions

1. "You" agree to use due care to prevent a "privacy breach". This includes, but is not limited to, adherence to industry, privacy, legal and regulatory standards for the protection of "data" from a "privacy breach" 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 "privacy breach" to "us" and/or applicable Provincial and/or Federal Privacy Regulators, law enforcement personnel, CYBERSCOUT, and/or other designated service providers;
4. Upon discovery of a "privacy breach", "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).

Definitions

1. **"Account Takeover"**: The unauthorized use of a person's existing financial account(s) or services.
2. **"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.
3. **"Data Subject":** An individual human being whose "Personal Information" is lost, stolen, improperly accessed, accidentally released or accidentally published due to a "privacy breach".
4. **"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".
5. **"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.
6. **"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).
7. **"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 "privacy breach" 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.
8. **"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.

    For "privacy breaches" necessitating provision of "monitoring services", an Internet based enrollment platform in addition to phone-in enrollment options will be offered.
9. **"Notification Recipient":** A "data subject" who is notified by "you" that "Personal Information (PI)" is exposed or potentially exposed to an unauthorized third party or multiple third parties through a "privacy 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.

10. **Notification Recipient Services**: “We” will provide the following services for a covered “privacy 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 (“Privacy Breach” Response Line) for “notification recipients” to call to address issues, questions or concerns regarding the “privacy breach”. This includes the assignment of a live, U.S. or Canadian 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 “fraud alert” for those who believe they are at risk of becoming or have become “identity fraud” victims.
11. **“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.
12. **“Privacy Breach”**: The loss, theft, accidental release, accidental publication of “data” involving one or more “data subjects”. This includes “privacy breach” 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.
13. **“We”, “Us”** and “**Our”:** The words “we”, “us” and “our” refer to the Company providing the insurance
14. **“You”** and “**Your”:** Throughout this endorsement, “you” and “your” refers to the Named Policyholder as defined within the insurance policy Declarations Page.