THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

PERSONAL CYBER COVERAGE - FORM 3204

Cyber Attack, Cyber Extortion, Online Fraud and Data Breach

This endorsement is added under SECTION I - OPTIONAL COVERAGES and is subject to all the terms and conditions applicable to SECTION I.

DEFINITIONS

Terms that appear in quotation marks but are not defined in this endorsement have definitions assigned to them in the policy wording to which this endorsement attaches.
Solely for the purposes of this endorsement, the following definitions are added:

1. "Affected individual" means any person whose "personally identifying information" is lost, stolen, accidentally released or accidentally published by a "data breach" covered under this endorsement. This definition is subject to the following provisions:
   a. "Affected individual" must be someone whose "personally identifying information" is in "your" possession because of:
      (1) A family or personal relationship with "you"; or
      (2) "Your" activities or responsibilities in connection with volunteer work for a non-profit organization.
   b. "Affected individual" does not mean or include any of the following:
      (1) "You";
      (2) Anyone whose "personally identifying information" is in "your" possession because of the activities or responsibilities of "you" in connection with a for-profit organization or in connection with a non-profit organization for which "you" are a paid employee or contract worker. Such organizations include, but are not limited to, organizations that "you" own or operate; or
      (3) Any business, organization or entity. Only an individual person may be an "affected individual".

2. "Computing device" means a desktop, laptop or tablet computer or wi-fi router or other Internet access point. Such device must be owned or leased by "you" and operated under "your" control.

3. "Connected home device" means any electronic device, other than a "computing device", that connects to the Internet or to other electronic devices. This includes, but is not limited to, networked versions of any of the following:
   a. Smart phones;
   b. Thermostats;
   c. Entertainment systems;
   d. Appliances;
   e. Smoke, fire and home security monitoring systems; or
   f. Cameras.
   Such device must be owned or leased by "you" and operated under "your" control.

4. "Cyber attack" means one of the following involving a "computing device" or "connected home device":
   a. Unauthorized Access or Use - meaning the gaining of access to "your" "computing device" or "connected home device" by an unauthorized person or persons or by an authorized person or persons for unauthorized purposes; or
   b. Malware Attack – meaning damage to "your" "computing device", "connected home device" or "data" arising from malicious code, including viruses, worms, Trojans, spyware and keyloggers. This does not mean damage from shortcomings or mistakes in legitimate electronic code or damage from code installed on "your" "computing device" or "connected home device" during the manufacturing process.

5. "Cyber extortion event" means one of the following involving a "computing device" or "connected home device":
   a. A demand for money or other consideration based on a credible threat to damage, disable, deny access to or disseminate content from "your" "computing device", "connected home device" or "data"; or
   b. A demand for money or other consideration based on an offer to restore access or functionality in connection with an attack on "your" "computing device", "connected home device", or "data".

6. “Cyber extortion response costs” means any payment as directed by the extortion threat, but only when that payment is:
   a. Incurred as a direct result of a “cyber extortion event” directed against “you” ; and
   b. Approved in advance by “us”. However, at “our” sole discretion, “we” may pay for “cyber extortion response costs” that were not approved in advance by “us” if “we” determine the following:
      (1) It was not practical for “you” to obtain “our” prior approval; and
      (2) If consulted at the time, “we” would have approved the payment.

7. “Data breach”
   a. “Data breach” means the loss, theft, accidental release or accidental publication of “personally identifying information” regarding one or more “affected individuals”. At the time of the breach, such information must be in:
      (1) “Your” care, custody or control; or
      (2) The care, custody or control of a professional entity with whom “you” have a contract and to whom “you” have entrusted the information.
   b. With respect to Data Breach coverage, if the date of the “data breach” as defined in a. above cannot be determined, such date shall be deemed to be the date “you” first become aware of the loss, theft, release or publication of the “personally identifying information”, provided that such date falls within the policy period.

8. “Data recovery costs”
   a. “Data recovery costs” means the costs of a professional firm hired by “you” to replace electronic “data” that has been lost or corrupted.
   b. “Data recovery costs” does not mean costs to research, re-create or replace any of the following:
      (1) Software programs or operating systems that are not commercially available;
      (2) “Data” that cannot reasonably be replaced. This includes, but is not limited to, personal photos, movies or recordings for which no back-up is available; or
      (3) “Data” that is obsolete, unnecessary or useless to “you”.

9. “Fraud costs” means the amount fraudulently taken from “you”. This is the direct financial loss only. “Fraud costs” does not include any of the following:
   a. Other expenses that arise from the “fraud event”;
   b. Indirect loss, such as “bodily injury”, lost time, lost wages, identity recovery expenses or damaged reputation;
   c. Any interest, time value or potential investment gain on the amount of financial loss; or
   d. Any portion of such amount that has been or can reasonably be expected to be reimbursed by a third party, such as a financial institution.

10. “Fraud event”
   a. “Fraud event” means any of the following, when such event results in direct financial loss to “you”:
      (1) An “identity theft”;
      (2) The unauthorized use of a card, card number or account number associated with a bank account or credit account issued to or registered in an “your” name, when “you” are legally liable for such use;
      (3) The forgery or alteration of any cheque or negotiable instrument;
      (4) Acceptance in good faith of counterfeit currency; or
      (5) An intentional and criminal deception of “you” to induce “you” to part voluntarily with something of value.

   b. “Fraud event” does not mean or include any occurrence:
      (1) In which “you” are threatened or coerced to part with something of value;
      (2) Between “you” and any of the following:
         (a) Any other “insured”;
         (b) “Your” current or former spouse, common law spouse or domestic partner; or
         (c) “Your” grandparent, parent, sibling, child or grandchild.
      (3) Involving use of a card, card number or account number associated with a bank account or credit account:
         (a) By a person who has ever received any authorization from “you” to use such card, card number or account number, unless such authorization was obtained through a criminal deception of “you”; or
         (b) If “you” have not complied with all terms and conditions under which such card, card number or account number was issued.
      (4) Arising from any of the following:
         (a) The business or professional service of an “insured”;
         (b) A dispute or a disagreement over the completeness, authenticity or value of a product, a service or a financial instrument;

(c) A gift or charitable contribution to an individual or any legitimate organization;
(d) An online auction or the use of an online auction site;
(e) A lottery, gambling or a game of chance; or
(f) An advance fee fraud or other fraud in which "you" provide money based on an expectation of receiving at some future time a larger amount of money or something with a greater value than the money provided.

11. "Identity theft" means the fraudulent use of "personally identifying information". This includes fraudulently using such information to establish credit accounts, secure loans, enter into contracts or commit crimes.

12. "One cyber occurrence" means all "cyber attacks", "cyber extortion events", "fraud events" and "data breaches" that:
    a. Take place at the same time; or
    b. Arise during the same policy period from the same source, cause or vulnerability.

13. "Personally identifying information"
    a. "Personally identifying information" means information that could be used to commit fraud or other illegal activity involving the credit or identity of an "affected individual". This information includes, but is not limited to, Social Insurance Numbers or other account numbers correlated with names or addresses.
    b. "Personally identifying information" does not mean or include information that is otherwise available to the public, such as names and addresses with no correlated or associated Social Insurance Numbers or other account numbers.

14. "System restoration costs"
    a. "System restoration costs" means the costs of a professional firm hired by "you" to do the following in order to restore "your" "computing device" or "connected home device" to the level of functionality it had before the "cyber attack":
        (1) Replace or reinstall "computer software" programs;
        (2) Remove any malicious code; and
        (3) Configure or correct the configuration of "your" "computing device" or "connected home device".
    b. "System restoration costs" does not mean any of the following:
        (1) Cost to repair or replace hardware. However, at "our" sole discretion, "we" may pay to repair or replace hardware if doing so reduces the amount of loss payable under this endorsement;
        (2) Cost to increase the speed, capacity or utility of "your" "computing device" or "connected home device";
        (3) Cost of "your" time or labour;
        (4) Any costs in excess of the replacement value of "your" "computing device" or "connected home device", including applicable hardware and software; nor
        (5) Cost to replace "computer software" programs or operating systems which are not commercially available.

COVERAGE

"We" will pay for the following subject to the Amount of Insurance stated in the Declarations unless otherwise specified below. Coverage provided under this endorsement does not increase any limit of liability under "your" policy.

SECTION 1 - CYBER ATTACK

CONDITIONS

This Cyber Attack coverage applies only if all of the following conditions are met:
1. There has been a "cyber attack"; and
2. Such "cyber attack" is first discovered by "you" during the policy period for which this endorsement is applicable; and
3. Such "cyber attack" is reported to "us" as soon as practicable, but in no event more than 60 days after the date it is first discovered by "you".

COVERAGE

If all of the conditions listed in the Cyber Attack CONDITIONS have been met, then "we" will provide "you" the following coverages for loss directly arising from such "cyber attack":
1. Data Recovery
   "We" will pay "your" necessary and reasonable "data recovery costs".

2. System Restoration
   "We" will pay "your" necessary and reasonable "system restoration costs".

SECTION 2 - CYBER EXTORTION

CONDITIONS

This Cyber Extortion coverage applies only if all of the following conditions are met:
1. There has been a "cyber extortion event" against "you"; and
2. Such "cyber extortion event" is first discovered by "you" during the policy period for which this endorsement is applicable; and
3. Such "cyber extortion event" is reported to "us" as soon as practicable, but in no event more than 60 days after the date it is first discovered by "you"; and
4. Such "cyber extortion event" is reported in writing by "you" to the police.

COVERAGE

If all of the conditions listed in the Cyber Extortion CONDITIONS have been met, then "we" will provide "you" with the following:
1. Professional assistance from a subject matter expert provided by "us" for advice and consultation regarding how best to respond to the threat; and
2. Reimbursement of "your" necessary and reasonable "cyber extortion response costs".

SECTION 3 - ONLINE FRAUD

CONDITIONS

This Online Fraud coverage applies only if all of the following conditions are met:
1. There has been a "fraud event" against "you" that is wholly or partially perpetrated through a "computing device" or "connected home device"; and
2. Such "fraud event" is first discovered by "you" during the policy period for which this endorsement is applicable; and
3. Such "fraud event" is reported to "us" as soon as practicable, but in no event more than 60 days after the date it is first discovered by "you"; and
4. Such "fraud event" is reported in writing by "you" to the police.

COVERAGE

If all of the conditions listed in the Online Fraud CONDITIONS have been met, then "we" will pay "your" necessary and reasonable "fraud costs".

SECTION 4 – DATA BREACH

CONDITIONS

This Data Breach coverage applies only if all of the following conditions are met:
1. There has been a "data breach" involving "personally identifying information"; and
2. Such "data breach" is first discovered by "you" during the policy period for which this endorsement is applicable; and
3. Such "data breach" is reported to "us" as soon as practicable, but in no event more than 60 days after the date it is first discovered by "you".

COVERAGE

If all of the conditions listed in the Data Breach CONDITIONS have been met, then “we” will provide “you” the following coverages for loss directly arising from such “data breach”:

1. Forensic IT Review
   “We” will pay the necessary and reasonable expense for a professional information technologies review, if needed, to determine within the constraints of what is possible and reasonable, the nature and extent of the “data breach” and the number and identities of the “affected individuals”.

   This does not include costs to analyze, research or determine any of the following:

   a. Vulnerabilities in systems, procedures or physical security;
   b. Compliance with security standards; or
   c. The nature or extent of loss or damage to “data” that is not “personally identifying information”.

   If there is reasonable cause to suspect that a covered “data breach” may have occurred, “we” will pay for costs covered under Forensic IT Review, even if it is eventually determined that there was no covered “data breach”. However, once it is determined that there was no covered “data breach”, “we” will not pay for any further costs.

2. Legal Review
   “We” will pay the necessary and reasonable expense for a professional legal counsel review, if needed, of the “data breach” and how “you” should best respond to it.

   If there is reasonable cause to suspect that a covered “data breach” may have occurred, “we” will pay for costs covered under Legal Review, even if it is eventually determined that there was no covered “data breach”. However, once it is determined that there was no covered “data breach”, “we” will not pay for any further costs.

3. Notification to Affected Individuals
   “We” will pay “your” necessary and reasonable costs to provide notification of the “data breach” to “affected individuals”.

4. Services to Affected Individuals
   This coverage only applies if “you” have provided notification of the “data breach” to “affected individuals” as covered under paragraph 3, Notification to Affected Individuals and in accordance with Additional Conditions 5, Pre-Notification Consultation.

   “We” will pay “your” necessary and reasonable costs to provide the following services to “affected individuals”.

   a. The following services apply to any “data breach”:
      1) Informational Materials
         packet of loss prevention and customer support information.
      2) Help Line
         toll-free telephone line for “affected individuals” with questions about the “data breach”. Where applicable, the line can also be used to request additional services as listed in b. 1) and 2).

   b. The following additional services apply to “data breaches” involving “personally identifying information”:
      1) Fraud Alert
      An alert placed on a credit file advising the creditor to validate the legitimacy of a credit application by contacting the “affected individual”. This service is initiated by the “affected individual” contacting the service provider who will provide assistance with placement of alerts with all designated Canadian credit bureaus.

      2) Identity Restoration Case Management
      Regarding any “affected individual” who is or appears to be a victim of “identity theft” that may reasonably have arisen from the “data breach”, the services of an identity restoration professional who will assist that “affected individual” through the process of correcting credit and other records and, within the constraints of what is possible and reasonable, restoring control over his or her personal identity.

LOSS OR DAMAGE NOT INSURED

The following additional exclusions apply to all coverages under this endorsement.

"We" will not pay for loss, damage or expense caused by or resulting from:

1. Any of the following by "you":
   a. Criminal, fraudulent or dishonest act, error or omission;
   b. Intentional violation of the law; or
   c. Intentional causing or contributing to a covered loss event;
2. Any criminal investigations or proceedings;
3. Any physical damage;
4. Any damage to a motor vehicle, watercraft, aircraft, or other vehicle.
5. Any third party liability or legal defense costs;
6. Any fines or penalties;
7. Loss to the Internet, an Internet service provider or any device or system that is not owned or leased by "you" and operated under "your" control;
8. Loss arising from any business, including but not limited to any business owned or operated by "you" or any business employing "you";
9. Except as specifically provided under the System Restoration portion of Cyber Attack coverage, costs to research or correct any deficiency;
10. Any "cyber attack", "cyber extortion event", "fraud event" or "data breach" first discovered by "you" prior to the inception of "your" coverage under this endorsement; or
11. Any "cyber attack", "cyber extortion event", "fraud event" or "data breach" first occurring more than 60 days prior to the inception of "your" coverage under this endorsement.

AMOUNT OF INSURANCE

The Home Cyber Protection Annual Aggregate Limit shown on the Declarations for this endorsement is the most "we" will pay under this endorsement for all loss, damage or expense arising during any one policy period. This limit shall apply to the total of all loss, damage or expense arising from all "cyber attacks", "cyber extortion events", "fraud events" or "data breaches" occurring during such policy period. "Our" costs under Section 2 – Cyber Extortion to provide you with professional assistance from a subject matter expert shall not count towards the loss, damage or expense included within "your" coverage limit.

If "one cyber occurrence" causes loss, damage or expense in more than one policy period, all such loss, damage and expense will be subject to the Personal Cyber Coverage Annual Aggregate Limit of the first policy period.

DEDUCTIBLE

"We" will only pay that part of the loss that exceeds the Personal Cyber Coverage deductible shown in the Declarations. No other deductible applies to this coverage.

ADDITIONAL CONDITIONS

1. **Confidentiality**
   With respect to Section 2 – Cyber Extortion, "you" must make every reasonable effort not to divulge the existence of this coverage to anyone other than the police.

2. **Due Diligence**
   "You" agree to use due diligence to prevent and mitigate costs covered under this endorsement. This includes, but is not limited to, complying with reasonable and widely-practiced steps for:
   a. Providing and maintaining appropriate system and "data" security; and
   b. Maintaining and updating at appropriate intervals, backups of electronic "data".

3. **Legal Advice**
   "We" are not "your" legal advisor. Our determination of what is or is not insured under this endorsement does not represent advice or counsel from "us" about what you should or should not do.

4. **Other Coverage**
If elements of coverage under this endorsement are covered under the policy to which this endorsement is attached or under any other policy in force at the time of a covered event, then coverage under this endorsement will apply as excess coverage only. If loss payment has been made under this or any other policy for the same event, the amount of such payment will count towards the deductible that applies to coverage under this endorsement.

5. **Pre-Notification Consultation**
   a. "You" agree to consult with "us" prior to the issuance of notification to "affected individuals" under Section 4 – Data Breach. "We" assume no responsibility for any services promised to "affected individuals" without "our" prior agreement.
   b. "We" will suggest a service provider for Notification to Affected Individuals and Services to Affected Individuals. If "you" prefer to use an alternate service provider, "our" coverage is subject to the following limitations:
      (1) Such alternate service provider must be approved by "us"; and
      (2) "Our" payment for services provided by any alternate service provider will not exceed the amount that "we" would have paid using the service provider "we" had suggested.
   c. "You" will provide us and the service provider the following at "our" pre-notification consultation with "you":
      (1) The exact list of "affected individuals" to be notified, including contact information;
      (2) Information about the "data breach" that may appropriately be communicated to "affected individuals"; and
      (3) The scope of services that "you" desire for the "affected individuals". For example, coverage may be structured to provide fewer services in order to make those services available to more "affected individuals" without exceeding the available limit of coverage.

6. **Services**
   a. "We" will only pay under this endorsement for services that are provided by service providers approved by "us". "You" must obtain "our" prior approval for any service provider whose expenses "you" want covered under this endorsement. "We" will not unreasonably withhold such approval.
   b. "You" will have a direct relationship with the professional service firms paid for in whole or in part under this endorsement. Those firms work for "you".
   c. With respect to any services provided by any service firm paid for in whole or in part under this endorsement:
      (1) The effectiveness of such services depends on "your" cooperation and assistance;
      (2) "We" do not warrant or guarantee that the services will end or eliminate all problems associated with the covered events;
      (3) "We" do not warrant or guarantee that services will be available or applicable to all individuals.

All other provisions of this policy apply.