

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

CYBER RISK PROTECTION - HOME COVERAGE

Cyber Attack, Cyber Extortion, Online Fraud, Data Breach and Identity Recovery

The following additional coverage is added to our base policy. Terms that appear in quotation marks but are not defined in this endorsement have the definitions assigned to them in the policy to which this endorsement attaches.

SCHEDULE

Coverage under this endorsement is subject to the limits and deductible indicated below.

| | |
|---|----------|
| Cyber Risk Protection - Home Annual Aggregate Limit (Applies per policy period to all coverages under Sections 1, 2, 3, and 4 of this endorsement) | \$25,000 |
| Cyber Risk Protection - Home Occurrence Deductible (Applies per occurrence to all coverages under Sections 1, 2, 3, and 4 of this endorsement) | \$ 500 |
| Identity Recovery Annual Aggregate Limit (Applies per policy period to all coverages under Section 5 of this endorsement) | \$25,000 |
| Identity Recovery Occurrence Deductible (Applies per occurrence to all coverages under Section 5 of this endorsement) | \$ 0 |

DEFINITIONS

The following definitions are added:

1. "Affected individual" means any person whose "personally identifying information" or "personally sensitive 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" or "personally sensitive information" is in your possession because of:
 - (1) A family or personal relationship with you or another "insured"; or
 - (2) The activities or responsibilities of you or another "insured" in connection with volunteer work for a non-profit organization.
 - b. "Affected individual" does not mean or include any of the following:
 - (1) You or another "insured".
 - (2) Anyone whose "personally identifying information" or "personally sensitive information" is in your possession because of the activities or responsibilities of you or another "insured" 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.
 - (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 or another "insured" as well as operated under your or another "insureds" 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 or another "insured" as well as operated under your or another "insureds" 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 device or system by an unauthorized person or persons or by an authorized person or persons for unauthorized purposes.
 - b. Malware Attack – meaning damage to your device, system or data arising from malicious code, including viruses, worms, Trojans, spyware and key loggers. This does not mean damage from shortcomings or mistakes in legitimate electronic code or damage from code installed on your computer system 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 device, system or data;
 - b. A demand for money or other consideration based on an offer to restore access or functionality in connection with an attack on your device, system 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 or another "insured"; and
 - b. Approved in advance by us. However, 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" or "personally sensitive information" as respects one or more "affected individuals". At the time of the breach, such information must be in the care, custody or control of:
 - (1) You or another "insured"; or
 - (2) A professional entity with whom you or another "insured" have a contract and to whom you or another "insured" have entrusted the information.
 - b. As respects 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" or "personally sensitive information".
8. "Data recovery costs"
 - a. "Data recovery costs" means the costs of a professional firm hired by you or another "insured" 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 electronic back-up is available.
 - (3) Data that is obsolete, unnecessary or no longer of use.
9. "Fraud costs" means the amount fraudulently taken from the "insured". 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 an "insured":
 - (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 "insured's" name, when the "insured" is legally liable for such use;
 - (3) The forgery or alteration of any check or negotiable instrument;
 - (4) Acceptance in good faith of counterfeit currency; or
 - (5) An intentional and criminal deception of an "insured" to induce the "insured" to part voluntarily with something of value.
 - b. "Fraud event" does not mean or include any occurrence:
 - (1) In which the "insured" is threatened or coerced to part with something of value;
 - (2) Between an "insured" and any of the following:
 - (a) Any other "insured";
 - (b) The "insured's" current or former spouse, common law spouse or domestic partner; or
 - (c) The "insured's" 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 an "insured" to use such card, card number or account number, unless such authorization was obtained through a criminal deception of the "insured"; or
 - (b) If an "insured" has 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.
 - (f) An advance fee fraud or other fraud in which an "insured" provides 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 recovery case manager" means one or more individuals assigned by us to assist an "insured" with communications we deem necessary for re-establishing the integrity of the personal identity of the "insured". This includes, with the permission and cooperation of the "insured", written and telephone communications with law enforcement authorities, governmental agencies, credit agencies and individual creditors and businesses.
12. "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.
13. "Identity theft costs" means the following when they are reasonable and necessary costs that are incurred as a result of an "identity theft":
 - a. Costs for re-filing applications for loans, grants or other credit instruments that are rejected solely as a result of an "identity theft".
 - b. Costs for long distance telephone calls, postage and notarizing documents;
 - c. Costs for credit reports from established credit bureaus;
 - d. Costs for an attorney approved by us for the following:
 - (1) The defense of any civil suit brought against an "insured";
 - (2) The removal of any civil judgment wrongfully entered against an "insured";
 - (3) Legal assistance for an "insured" at an audit or hearing by a governmental agency;
 - (4) Legal assistance in challenging the accuracy of the "insured's" consumer credit report; or
 - (5) The defense of any criminal charges brought against an "insured" arising from the actions of a third party using the personal identity of the "insured".
 - e. Actual lost wages of the "insured" for time taken away from work and from the work premises. Time away from work includes partial or whole work days. Actual lost wages may include payments days, discretionary days, floating holidays and paid personal days does not include sick days or any loss arising from time taken away from self-employment. Necessary time off does not include time off to do tasks that could reasonably have been done during non-working hours;
 - f. Costs of supervision of children or elderly or infirm relatives or dependents of the "insured" during time taken away from such supervision. Such care must be provided by a professional care provider who is not a relative of the "insured".
 - g. Costs for counseling from a licensed mental health professional. Such care must be provided by a professional care provider who is not a relative of the "insured."
 - h. Any other reasonable costs necessarily incurred by an "insured" as a direct result of the "identity theft".
 - (1) Such costs include:
 - (a) Costs by the "insured" to recover control over his or her personal identity.
 - (b) Deductibles or service fees from financial institutions.
 - (2) Such costs do not include:
 - (a) Costs to avoid, prevent or detect "identity theft" or other loss.
 - (b) Money lost or stolen.
 - (c) Costs that are restricted or excluded elsewhere in this endorsement or policy.
14. "One cyber occurrence" means all "cyber attacks", "cyber extortion events", "data breaches", and "fraud events" that:
 - a. Take place at the same time; or
 - b. Arise during the same Policy Period from the same source, cause or vulnerability.
15. "Personally identifying information"
 - a. "Personally identifying information" means information, including health information, which could be used to commit fraud or other illegal activity involving the credit, access to health care or identity of an "affected individual". This includes, but is not limited to, Social Security numbers or account numbers.

- b. "Personally identifying information" does not mean or include information that is otherwise available to the public, such as names and addresses.
16. "Personally sensitive information" means private information specific to an individual the release of which requires notification of "affected individuals" under any applicable law.
17. "System restoration costs"
- a. "System restoration costs" means the costs of a professional firm hired by you or another "insured" 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 device or system.
 - b. "System restoration costs" does not mean any of the following:
 - (1) Costs 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) Costs to increase the speed, capacity or utility of your device or system.
 - (3) Your time or labor.
 - (4) Any costs in excess of the replacement value of your system, including applicable hardware and software.

COVERAGE AGREEMENT

We will provide the insurance described in this endorsement in compliance with all applicable provisions (including but not limited to, Conditions, Definitions and Exclusions) of your Homeowners policy. Coverage provided under this endorsement does not increase any limit of liability under your Homeowners policy.

SECTION 1 – CYBER ATTACK

SECTION 1 – COVERAGE REQUIREMENTS

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 or another "insured" 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 or another "insured".

SECTION 1 – COVERAGES PROVIDED

If all of the conditions listed above in SECTION 1 – COVERAGE REQUIREMENTS 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

SECTION 2 – COVERAGE REQUIREMENTS

This Cyber Extortion coverage applies only if all of the following conditions are met:

1. There has been a “cyber extortion event” against you or another “insured”; and
2. Such “cyber extortion event” is first discovered by you or another “insured” 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.

SECTION 2 – COVERAGES PROVIDED

If all of the conditions listed above in SECTION 2 – COVERAGE REQUIREMENTS 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.
2. Reimbursement of your necessary and reasonable “cyber extortion response costs”.

SECTION 3 – ONLINE FRAUD

SECTION 3 – COVERAGE REQUIREMENTS

This Online Fraud coverage applies only if all of the following conditions are met:

1. There has been a “fraud event” against you or another “insured” that is wholly or partially perpetrated through a “computing device” or “connected home device”; and
2. Such “fraud event” is first discovered by you or another “insured” 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 or another “insured” to the police.

SECTION 3 – COVERAGES PROVIDED

If all of the conditions listed above in SECTION 3 – COVERAGE REQUIREMENTS have been met, then we will pay your necessary and reasonable “fraud costs”.

SECTION 4 – DATA BREACH

SECTION 4 – COVERAGE REQUIREMENTS

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” or “personally sensitive 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.

SECTION 4 – COVERAGES PROVIDED

If all of the conditions listed above in SECTION 4 – COVERAGE REQUIREMENTS have been met, then we will provide you the following coverages for loss directly arising from such “data breach”.

1. Forensic IT Review

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” or “personally sensitive 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

Professional legal counsel review 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 above.

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
A packet of loss prevention and customer support information.
 - 2) Help Line

A 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) Credit Report and Monitoring

A credit report and an electronic service automatically monitoring for activities affecting an individual’s credit records. This service is subject to the “affected individual” enrolling for this service with the designated service provider.

2) Identity Restoration Case Management

As respects 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.

SECTION 5 – IDENTITY RECOVERY

SECTION 5 – COVERAGE REQUIREMENTS

This Identity Recovery coverage applies only if all of the following conditions are met:

1. There has been an “identity theft” involving the personal identity of an “insured”; and
2. Such “identity theft” is first discovered by you during the policy period for which this endorsement is applicable; and
3. Such “identity theft” 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.
4. Such “identity theft” is reported in writing by you or another “insured” to the police.

SECTION 5 – COVERAGES PROVIDED

If all of the conditions listed above in SECTION 5 – COVERAGE REQUIREMENTS have been met, then we will provide you the following coverages for loss directly arising from such “identity theft”.

1. Case Management Service

We will provide the services of an “identity recovery case manager” as needed to respond to the “identity theft”.

2. Costs Coverage

We will pay your reasonable and necessary “identity theft costs”.

EXCLUSIONS

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 or any insured:

- 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, and any device or system that is not owned or leased by you or another "insured" and operated under your or another "insureds" control.
 8. Loss arising from any business, including but not limited to any business owned or operated by any "insured" or any business employing any "insured".
 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", "data breach", "fraud event" or "identity theft" first discovered by you prior to the inception of your coverage under this endorsement.
 11. Any "cyber attack", "cyber extortion event", "data breach", "fraud event" or "identity theft" first occurring more than 60 days prior to the inception of your coverage under this endorsement.
 12. The theft of a professional or business identity.
-

LIMITS

The Home Cyber Protection Annual Aggregate Limit shown in the Schedule is the most we will pay under Sections 1, 2, 3 and 4 of this endorsement for all loss, damage or expense arising during any one policy year. This limit shall apply to the total of all loss, damage or expense arising from all "cyber attacks", "cyber extortion events", "data breaches" or "fraud events" occurring during such policy year. 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 year, all such loss, damage and expense will be subject to the Home Cyber Protection Annual Aggregate Limit of the first such policy year.

The Identity Recovery Annual Aggregate Limit shown in the Schedule is the most we will pay for the total of all loss or expense arising out of all "identity thefts" to any one "insured" which are first discovered by the "insured" during the present annual policy period. Case Management Service under Section 5 – Identity Recovery is available as needed for any one "identity theft" for up to 12 consecutive months from the inception of the service. Costs we incur to provide Case Management Service do not reduce the amount of limit available for Costs Coverage.

Costs Coverage under Section 5 – Identity Recovery is subject to the limit shown in the schedule. If an "identity theft" is first discovered in one policy period and continues into other policy periods, all loss and expense arising from such "identity theft" will be subject to the aggregate limit applicable to the policy period when the "identity theft" was first discovered.

Legal costs as provided under item d. of the definition of "identity theft costs" are part of, and not in addition to, the Costs Coverage limit.

Item e. (Lost Wages) and item f. (Child and Elder Care Expenses) of the definition of "identity theft costs" are jointly subject to a sublimit of \$5,000. This sublimit is part of, and not in addition to, the Costs Coverage limit. Coverage is limited to wages lost and costs incurred within 12 months after the first discovery of the "identity theft" by the "insured."

Item g. (Mental Health Counseling) of the definition of “identity theft costs” is subject to a sublimit of \$1,000. This sublimit is part of, and not in addition to, the Costs Coverage limit. Coverage is limited to costs incurred within 12 months after the first discovery of the “identity theft” by the “insured.”

Item h. (Miscellaneous Unnamed Costs) of the definition of “identity theft costs” is subject to a sublimit of \$1,000. This sublimit is part of, and not in addition to, the Costs Coverage limit. Coverage is limited to costs incurred within 12 months after the first discovery of the “identity theft” by the “insured.”

DEDUCTIBLES

Under Sections 1, 2, 3, and 4, we will not pay for loss, damage or expense arising from any “one cyber occurrence” until the amount of the covered loss, damage or expense exceeds the Home Cyber Protection Occurrence Deductible amount indicated in the Schedule for this endorsement. We will then pay the amount of loss, damage or expense in excess of the applicable deductible amount, subject to the Home Cyber Protection Annual Aggregate Limit.

Section 5 of this endorsement is not subject to a deductible.

CONDITIONS

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

1. **Assistance and Claims**

As respects Section 5 – Identity Recovery, for assistance the “insured” should call the **Identity Recovery Help Line** at **1-800-945-9313**.

The **Identity Recovery Help Line** can provide the “insured” with:

- a. Information and advice for how to respond to a possible “identity theft”; and
- b. Instructions for how to submit a service request for Case Management Service and/or a claim form for Costs Coverage.

In some cases, we may provide Case Management services at our expense to an “insured” prior to a determination that a covered “identity theft” has occurred. Our provision of such services is not an admission of liability under the policy. We reserve the right to deny further coverage or service if, after investigation, we determine that a covered “identity theft” has not occurred.

As respects Costs Coverage, the “insured” must send to us, within a 60 days after our request, receipts, bills or other records that support his or her claim for “identity theft costs”.

2. **Confidentiality**

As respects Section 2 – Cyber Extortion, “insureds” must make every reasonable effort not to divulge the existence of this coverage.

3. **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.

4. **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.

5. **Other Coverage in This Policy**

Some elements of coverage under this endorsement may also be covered under the policy to which this endorsement is attached. If so, the coverage under this endorsement will apply as excess, additional coverage. If loss payment has been made under the policy for the same event, the amount of such payment will count towards the deductible that applies to coverage under this endorsement.

6. **Pre-Notification Consultation**

- a. You agree to consult with us prior to the issuance of notification to “affected individuals” under Section 3 – 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 with “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.

5. **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 service providers paid for in whole or in part under this endorsement. Those firms work for you.
- c. As respects any services provided by any service providers 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 services will be available or applicable to all individuals.
 - (3) We do not warrant or guarantee that the services will end or eliminate all problems associated with the covered events.
 - (4) All services may not be available or applicable to all individuals. For example, under Section 5 – Identity Recovery “insureds” who are minors or foreign nationals may not have credit records that can be provided or monitored. Service in Canada will be different from service in the United States and Puerto Rico in accordance with local conditions.

All other provisions of this policy apply.