

PERSONAL CYBERPLUS® COVERAGE PART

THE LIMITS OF INSURANCE SHOWN IN THE PERSONAL CYBERPLUS® SCHEDULE (SCHEDULE) WILL BE REDUCED AND MAY BE COMPLETELY EXHAUSTED BY ALL AMOUNTS PAID UNDER THIS COVERAGE PART, INCLUDING DEFENSE COSTS.

PLEASE READ THE ENTIRE FORM CAREFULLY.

PERSONAL CYBERPLUS® SCHEDULE

Insurance is provided only if a specific Limit of Insurance is shown below:	Limit of Insurance
Personal CyberPlus® First Party Loss Coverage: (Event discovered and reported coverage)	\$
Personal CyberPlus® Privacy and Security Claims Coverage: (Claims-made and reported coverage)	\$
Combined Aggregate Limit:	\$

(The required information may be shown in the Schedule or in the Declarations)

NOTICE TO POLICYHOLDER

This Personal CyberPlus® Coverage Part forms a part of your Homeowners Policy (the Policy). Personal CyberPlus® Insurance is subject to its own terms, conditions, definitions, exclusions, limits and other provisions, as set forth herein, and except as it expressly states, this Coverage Part does not modify any of the terms and provisions of the Policy.

SECTION I. – PERSONAL CYBERPLUS® INSURANCE

Personal CyberPlus® First Party Loss Coverage

1. Insuring Agreements

a. Identity Theft Expenses Coverage

Subject to the Personal CyberPlus® First Party Loss Coverage Limit of Insurance, “we” shall reimburse “you” for “identity theft expenses” that “you” incur solely and directly because of “identity theft”, provided always that:

- (1) “you” first discover the “identity theft” during the “policy period”; and
- (2) “you” or “your” representatives report the “identity theft” to “us” as soon as practicable during the “policy period”, but no later than 60 days after the expiration or termination of the “policy period”.

b. Data Recovery & System Restoration Coverage

Subject to the Personal CyberPlus® First Party Loss Coverage Limit of Insurance, “we” shall reimburse “you” for “data recovery expenses” and “system restoration costs” that “you” incur solely and directly because of a “hacking attack”, provided always that:

- (1) “you” first discover the “hacking attack” during the “policy period”;
- (2) “you” or “your” representatives report the “hacking attack” to “us” as soon as practicable during the “policy period”, but no later than 60 days after the expiration or termination of the “policy period”; and
- (3) “you” provide clear evidence that the “data recovery expenses” and “system restoration costs” directly result from a “hacking attack”.

“We” shall reimburse “you” for “data recovery expenses” and “system restoration costs” for up to 12 months following “your” discovery of the “hacking attack”.

c. Credit Card Fraud & Forgery Coverage

Subject to the Personal CyberPlus® First Party Loss Coverage Limit of Insurance, “we” shall reimburse “you” for the loss of “money” that “you” sustain solely and directly because of “credit card fraud” or “forgery”, provided always that:

- (1) “you” first discover the “credit card fraud” or “forgery” during the “policy period”;
- (2) “you” or “your” representatives report the “credit card fraud” or “forgery” to “us” as soon as practicable during the “policy period”, but no later than 60 days after the expiration or termination of the “policy period”;
- (3) “you” notify “your” credit card company or bank of the facts and circumstances surrounding the “credit card fraud” or “forgery” as soon as practicable; and
- (4) “you” provide written confirmation to “us” that “your” credit card company or bank has refused to reverse or prevent a payment transaction, or to indemnify or reimburse “you” for the loss of “money”.

d. Cyber Crime Coverage

Subject to the Personal CyberPlus® First Party Loss Coverage Limit of Insurance, “we” shall reimburse “you” for “financial fraud loss” that “you” sustain solely and directly because of a “cyber crime event”, provided always that:

- (1) “you” first discover the “cyber crime event” during the “policy period”;
- (2) “you” or “your” representatives report the “cyber crime event” to “us” as soon as practicable during the “policy period”, but no later than 60 days after the expiration or termination of the “policy period”; and
- (3) “you” provide written confirmation to “us” that “your” bank has refused to reverse or prevent a payment transaction, or to indemnify or reimburse “you” for the “financial fraud loss”.

e. Cryptocurrency Crime Coverage

Subject to the Personal CyberPlus® First Party Loss Coverage Limit of Insurance, we shall reimburse “you” for the loss of “cryptocurrency” that “you” sustain solely and directly because of a “cryptocurrency crime event”, provided always that:

- (1) “you” first discover the “cryptocurrency crime event” during the “policy period”;
- (2) “you” or “your” representatives report the “cryptocurrency crime event” to “us” as soon as practicable during the “policy period”, but no later than 60 days after the expiration or termination of the “policy period”; and
- (3) “you” provide written confirmation to “us” that “your” “cryptocurrency exchange” has refused to reverse or prevent a payment transaction, or to indemnify or reimburse “you” for the loss of “cryptocurrency”.

f. Cyber Extortion Coverage

Subject to the Personal CyberPlus® First Party Loss Coverage Limit of Insurance, “we” shall reimburse “you” for “cyber extortion expenses” and “cyber extortion monies” that “you” incur solely and directly because of a “cyber extortion threat”, provided always that:

- (1) “you” first discover the “cyber extortion threat” during the “policy period”;
- (2) “you” or “your” representatives report the “cyber extortion threat” to “us” as soon as practicable during the “policy period”, but no later than 60 days after the expiration or termination of the “policy period”; and
- (3) “you” make every reasonable effort to notify local law enforcement authorities and the Federal Bureau of Investigation before surrendering any “cyber extortion monies” in response to a “cyber extortion threat”.

g. Cyber Bullying Coverage

Subject to the Personal CyberPlus® First Party Loss Coverage Limit of Insurance, “we” shall reimburse “you” for “cyber bullying expenses” that “you” incur solely and directly because of a “cyber bullying incident”, provided always that:

- (1) “you” first discover the “cyber bullying incident” during the “policy period”; and
- (2) “you” or “your” representatives report the “cyber bullying incident” to “us” as soon as practicable during the “policy period”, but no later than 60 days after the expiration or termination of the “policy period”.

h. Breach Notification Costs Coverage

Subject to the Personal CyberPlus® First Party Loss Coverage Limit of Insurance, “we” shall reimburse “you” for “breach notification costs” that “you” incur solely and directly because of a “security breach” or “privacy breach”, provided always that:

- (1) “you” first discover the “security breach” or “privacy breach” during the “policy period”; and
- (2) “you” or “your” representatives report the “security breach” or “privacy breach” to “us” as soon as practicable during the “policy period”, but no later than 60 days after the expiration or termination of the “policy period”.

2. Free Choice of Attorneys and Service Providers

- a. "You" shall have complete freedom of choice in the selection of "attorneys" and/or service providers to assist "you" in any "insured event". However, reimbursement of any costs, fees or charges of any "attorney" or service provider shall be limited to a maximum hourly rate of \$400.
- b. "You" will have a direct relationship with any "attorney" or service provider "you" retain, whether paid for in whole or in part under this Coverage Part. All "attorneys" and service providers work for "you".

3. Exclusions Applicable to the Personal CyberPlus® First Party Loss Coverage

The following Exclusions apply to all Insuring Agreements of the Personal CyberPlus® First Party Loss Coverage.

The Personal CyberPlus® First Party Loss Coverage does not apply to, and "we" have no obligation under the Personal CyberPlus® First Party Loss Coverage to pay for:

- a. any amounts incurred by "you" in disputes with respect to this insurance, including questions as to whether amounts are reimbursable under this Coverage Part.
- b. any costs to replace or repair any property, hardware or "connected device"; however, at "our" sole discretion, "we" may pay to replace or repair any property, hardware or "connected device" if doing so reduces the amount of "first party loss" reimbursable under this Coverage Part.
- c. any amounts incurred by "you" to institute legal proceedings against any person or organization.
- d. any "first party loss" arising from a false report of an "insured event" made by "you", whether acting alone or in collusion with others; however, this Exclusion does not apply to any "insured" who did not commit, participate in, or have prior knowledge of any conduct to which this Exclusion would otherwise apply.
- e. any "first party loss" arising from any willful, intentional, malicious, fraudulent, dishonest or criminal act or intentional violation of law, including any willful or intentional "privacy breach", committed by an "insured", whether acting alone or in collusion with others; however, this Exclusion does not apply to any "insured" who did not commit, participate in, or have prior knowledge of any conduct to which this Exclusion would otherwise apply.
- f. any "first party loss" incurred by "your" former spouse or "domestic partner", or a "family member" who is no longer residing with "you".
- g. any "first party loss" arising from:
 - (1) fire, smoke, explosion, leakage, lightning, wind, water, flood (including waves, tidal waves, or the rising or overflow of, or breaking out of, a body of water, whether natural or manmade), earthquake, volcanic eruption, landslide, hail, extreme weather, force majeure, or any other natural or physical event, however caused;
 - (2) any actual, alleged or threatened presence of pollutants or contamination of any kind, including, but not limited to, asbestos, vapor, soot, fumes, acids, alkalis, chemicals and waste ("waste" includes materials to be recycled, reconditioned or reclaimed), whether or not such presence results from an "insured's" activities or the activities of others, or such presence or contamination happened suddenly or gradually, accidentally or intentionally, or expectedly or unexpectedly; or
 - (3) any directive or request to test for, monitor, clean up, remove, contain, treat, detoxify or neutralize pollutants, or in any way respond to, or assess the effects of, pollutants or contamination of any kind.
- h. any "first party loss", cost or expense:
 - (1) directly or indirectly caused by, resulting from or in connection with any "war";
 - (2) resulting from a "cyber operation" carried out as part of any "war"; or
 - (3) resulting from a "cyber operation" that causes a sovereign state to become an "impacted state".

However, paragraph (3) above shall not apply to the direct or indirect effect of a "cyber operation" on a "covered device" that is not physically located in an "impacted state" but is affected by a "cyber operation".
- i. any "insured event" which was known to any "insured" prior to the "policy period".
- j. physical damage or injury to, or impairment, destruction or corruption of, any tangible property, including the loss of use thereof.
- k. any damage to a motor vehicle, watercraft, aircraft or other vehicle.
- l. any "first party loss" arising from a breach of, or liability assumed by an "insured" under, any written or oral contract or agreement.

- m.** any “first party loss” arising from any activities of, or relating to, a “business” owned or operated by “you”; or any “insured’s” activities as a stockholder, owner, manager, agent, partner, officer, director, paid employee or contractor of any for-profit or non-profit organization.
- n.** any “first party loss” arising from “your” civic or public activities, including “your” pursuit or holding of any public office; however, this Exclusion does not apply to a “privacy breach” directly resulting from such activities.
- o.** any “first party loss” arising from illness, substance abuse or death.
- p.** any costs to comply with any order, grant or agreement to provide non-monetary relief.
- q.** any “business identity theft”.
- r.** any “first party loss” arising from any electrical or mechanical surge, failure or interruption, including electrical disturbance, spike, brownout or blackout; or a total, partial, temporary or intermittent outage, failure, disruption or reduction in supply of any utility service or infrastructure, including electricity, gas, water, telephone, cable, internet, satellite or telecommunications, or any failure, outage, disruption, degradation or termination of any critical part of such service or infrastructure.
- s.** any fines, penalties, taxes or sanctions imposed by law, or any matters deemed uninsurable under applicable law.
- t.** any judgments, awards or settlement amounts “you” are legally obligated to pay to a “third party”.
- u.** “criminal proceedings”; however, this Exclusion does not apply to “identity theft expenses” incurred to remove criminal judgments wrongly entered against “you” as a result of “identity theft”.
- v.** retainers or any advanced costs.
- w.** any amounts “you” have paid, or agree to pay, as part of any service or maintenance contract, including a computer system maintenance contract.
- x.** any “first party loss” arising from errors or shortcomings in legitimate electronic code or code installed on a “connected device” during the manufacturing process.
- y.** any “first party loss” arising from any “connected device” that has had its software altered from the original manufactured state (also known as jailbroken).
- z.** any amounts to retrieve, replace, recreate or restore any “business” records or “business”-related data, including any such data or records that is stored on a “connected device”.
- aa.** any income loss caused by or resulting from “unauthorized trading”.
- bb.** “your” loss of “cryptocurrency” arising from:
 - (1)** an outage, interruption, failure, suspension or degradation of service of a computer system owned, controlled, leased or operated by a “cryptocurrency exchange”;
 - (2)** the theft of “cryptocurrency” or “private keys” in a network attack perpetrated against a computer system owned, controlled, leased or operated by a “cryptocurrency exchange”, including a “denial of service attack” or infection of such computer system by a “virus”, which attack impacts more than one customer of the “cryptocurrency exchange”; or
 - (3)** the insolvency or bankruptcy of any “cryptocurrency exchange”.
- cc.** any “first party loss” caused by or resulting from the use of a credit, debit or bank card or card number, password, PIN or other security code, or account number associated with a bank account, credit account, brokerage account, investment account or “cryptocurrency” account:
 - (1)** by any person or organization, whether acting alone or in collusion with others, who has ever been authorized by an “insured” to use such card, card number, password, PIN, security code, or account number; however, this Exclusion will not apply to “financial fraud loss” resulting from authorization obtained through deception of an “insured” in a “phishing attack”;
 - (2)** if an “insured” has not complied with all terms and conditions under which such card, card number or account number was issued; or
 - (3)** in connection with the operation of any “business”.
- dd.** any amounts that have been wholly or partially reversed, or reimbursed to “you”, by a credit card company, bank or “cryptocurrency exchange”.
- ee.** “your” loss of “other property” arising out, resulting from, or involving the fraudulent or purportedly fraudulent use of a credit or debit card.

- ff. any “first party loss” caused by or resulting from the giving or surrendering of “money”, “cryptocurrency”, “securities” or “other property” in any exchange for, or purchase of, goods or services:
 - (1) that are not yet delivered, whether fraudulent or not;
 - (2) that fail to conform to advertised quality or performance; or
 - (3) that fail to conform to the quality or performance expected from the standpoint of the “insured”.
- gg. “your” indirect costs, such as lost time, lost wages, damaged reputation, or potential income, including interest and dividends, not being realized; or any time value or potential investment gain on the amount of “money”, “securities” or “cryptocurrency” fraudulently taken from “you”; however, this Exclusion does not apply to lost wages directly resulting from “identity theft” or a “cyberbullying incident”.
- hh. any “first party loss” arising from the theft or loss of “cryptocurrency” or a “private key” that is held on any hardware, physical device, or other physical medium.
- ii. any “first party loss” arising from an “operating system event”.
- jj. any “first party loss” arising from a “widespread event”. The determination of whether an event constitutes a “widespread event” will rely upon any available evidence such as information from governments, news media, qualified IT forensics firms, computer experts and claims reported to “us”.
- kk. any amounts to which the Personal CyberPlus® Privacy and Security Claims Coverage applies.

Personal CyberPlus® Privacy and Security Claims Coverage

1. Insuring Agreement

Subject to the Personal CyberPlus® Privacy and Security Claims Coverage Limit of Insurance, “we” shall reimburse “you” for “damages” and reasonable and necessary “defense costs” that “you” become legally obligated to pay as a result of a “privacy and security claim”, provided always that:

- a. the “privacy and security claim” is first made against “you” during the “policy period”;
- b. “you” or “your” representatives report the “privacy and security claim” to “us” as soon as practicable during the “policy period”, but no later than 60 days after expiration or termination of the “policy period”; and
- c. the actual or alleged acts, events or incidents giving rise to the “privacy and security claim” first occur on or after the inception date of the first Personal CyberPlus® Coverage Part issued by “us” to the “named insured”.

2. No Duty to Defend; Free of Choice of Counsel

- a. “We” shall have no duty to defend any “privacy and security claim”, but only to reimburse “you” for “defense costs” and “damages”. The obligation to defend any “privacy and security claim” resides solely with “you”, and “your” reasonable and good faith defense of any “privacy and security claim” is a condition precedent to coverage under the Personal CyberPlus® Privacy and Security Claims Coverage.
- b. “We” shall reimburse “you” only for “defense costs” incurred for actual services rendered and/or “damages” sustained against “you” in a “privacy and security claim”, up to the applicable Limit of Insurance. However, actual payment by “you” of “defense costs” or “damages” will not be a condition precedent to reimbursement.
- c. “You” shall have complete freedom of choice in the selection of an “attorney” to represent “you” in any “privacy and security claim”. However, reimbursement of “defense costs” shall be limited to a maximum hourly “attorney” rate of \$400. “You” will have a direct relationship with any “attorney” retained by “you”.

3. Exclusions Applicable to the Personal CyberPlus® Privacy and Security Claims Coverage

The following Exclusions apply to the Personal CyberPlus® Privacy and Security Claims Coverage.

Personal CyberPlus® Privacy and Security Claims Coverage does not apply to, and “we” have no obligation under the Personal CyberPlus® Privacy and Security Claims Coverage to pay for:

- a. any amounts incurred by “you” in disputes with respect to this insurance, including questions as to whether amounts are reimbursable under this Coverage Part.
- b. any amounts incurred by “you” to institute legal proceedings against any person or organization.
- c. any “privacy and security claim” for, based upon, arising from or involving any acts, events or incidents which were known to any “insured” prior to the inception date of the first Personal CyberPlus® Coverage Part issued by “us” to the “named insured”.

- d. any matter brought against “you” for physical damage or injury to, or impairment, destruction or corruption of, any tangible property, including the loss of use thereof.
- e. any matter brought against “you” for damage to a motor vehicle, watercraft, aircraft or other vehicle.
- f. any matter brought against “you” for physical injury, sickness, disease or death sustained by any person, and where resulting from such physical injury only, mental anguish, mental injury, shock, humiliation or emotional distress.
- g. any “privacy and security claim” for, based upon, arising from or involving any liability assumed by an “insured” under, or breach of, any written or oral contract or agreement; however, this Exclusion does not apply to any liability “you” would have had in the absence of such contract or agreement and which would have been insured under the Personal CyberPlus® Privacy and Security Claims Coverage.
- h. any “privacy and security claim” for, based upon, arising from or involving any activities of, or relating to, a “business” owned or operated by “you”; or any “insured’s” activities as a stockholder, owner, manager, agent, partner, officer, director, paid employee or contractor of any for-profit or non-profit organization.
- i. any “privacy and security claim” for, based upon, arising from or involving “your” civic or public activities, including “your” pursuit or holding of any public office; however, this Exclusion does not apply to a “privacy and security claim” alleging a “privacy breach” directly resulting from such activities.
- j. any “privacy and security claim” for, based upon, arising from or involving any willful, intentional, malicious, fraudulent, dishonest or criminal act or intentional violation of law, including any willful or intentional “privacy breach”, committed by an “insured”, whether acting alone or in collusion with others, however, this Exclusion does not apply to any “insured” who did not commit, participate in, or have prior knowledge of any conduct to which this Exclusion would otherwise apply.
- k. any “privacy and security claim” for, based upon, arising from or involving:
 - (1) fire, smoke, explosion, leakage, lightning, wind, water, flood (including waves, tidal waves, or the rising or overflow of, or breaking out of, a body of water, whether natural or manmade), earthquake, volcanic eruption, landslide, hail, extreme weather, force majeure, or any other natural or physical event, however caused;
 - (2) any actual, alleged or threatened presence of pollutants or contamination of any kind, including, but not limited to, asbestos, vapor, soot, fumes, acids, alkalis, chemicals and waste (“waste” includes materials to be recycled, reconditioned or reclaimed), whether or not such presence results from an “insured’s” activities or the activities of others, or such presence or contamination happened suddenly or gradually, accidentally or intentionally, or expectedly or unexpectedly; or
 - (3) any directive or request to test for, monitor, clean up, remove, contain, treat, detoxify or neutralize pollutants, or in any way respond to, or assess the effects of, pollutants or contamination of any kind.
- l. any “damages”, cost or expense:
 - (1) directly or indirectly caused by, resulting from or in connection with any “war”;
 - (2) resulting from a “cyber operation” carried out as part of any “war”; or
 - (3) resulting from a “cyber operation” that causes a sovereign state to become an “impacted state”.

However, paragraph (3) above shall not apply to the direct or indirect effect of a “cyber operation” on a “covered device” that is not physically located in an “impacted state” but is affected by a “cyber operation”.
- m. any “privacy and security claim” for, based upon, arising from or involving any electrical or mechanical surge, failure or interruption, including electrical disturbance, spike, brownout or blackout; or a total, partial, temporary or intermittent outage, failure, disruption or reduction in supply of any utility service or infrastructure, including electricity, gas, water, telephone, cable, internet, satellite or telecommunications, or any failure, outage, disruption, degradation or termination of any critical part of such service or infrastructure.
- n. any costs to comply with any order, grant or agreement to provide non-monetary relief.
- o. any fines, penalties, taxes or sanctions, or any matters deemed uninsurable under applicable law.
- p. any punitive, exemplary, liquidated or multiplied damages; however, if a “privacy and security claim” is made against an “insured” seeking both compensatory and punitive, exemplary, liquidated or multiplied damages, then “we” will reimburse “defense costs” incurred in such “privacy and security claim” without liability for punitive, exemplary, liquidated or multiplied damages.
- q. any “privacy and security claim” made by or on behalf of an “insured” against another “insured”.
- r. “criminal proceedings”.

- s. retainers or any advanced costs.
- t. any amounts “you” have paid or agree to pay as part of any service or maintenance contract, including a computer system maintenance contract.
- u. any “privacy and security claim” for, based upon, arising from or involving a “widespread event”. The determination of whether an event constitutes a “widespread event” will rely upon any available evidence such as information from governments, news media, qualified IT forensics firms, computer experts and claims reported to “us”.
- v. any amounts to which the Personal CyberPlus® First Party Loss Coverage applies.

SECTION II. – LIMITS OF INSURANCE

The Limits of Insurance shown in the Schedule and the rules below fix the most “we” will pay under this Coverage Part, regardless of the number of “insureds”, “insured events” or “privacy and security claims”.

1. Personal CyberPlus® First Party Loss Coverage Limit of Insurance

The Personal CyberPlus® First Party Loss Coverage Limit of Insurance shown in the Schedule is the most “we” will reimburse under the Personal CyberPlus® First Party Loss Coverage for all “first party loss” arising from any one “insured event” first discovered during the “policy period”, and in the aggregate for all “insured events” first discovered during the “policy period”, regardless of the number of “insured events”, “insureds” or Insuring Agreements. All “first party loss” paid under the Personal CyberPlus® First Party Loss Coverage Limit of Insurance will reduce, and may completely exhaust, the Combined Aggregate Limit shown in the Schedule.

2. Personal CyberPlus® Privacy and Security Claims Limit of Insurance

The Personal CyberPlus® Privacy and Security Claims Coverage Limit of Insurance shown in the Schedule is the most “we” will reimburse under the Personal CyberPlus® Privacy and Security Claims Coverage for all “defense costs” and “damages” arising from any one “privacy and security claim” first made during the “policy period”, and in the aggregate for all “privacy and security claims” first made during the “policy period”, regardless of the number of “privacy and security claims”, “insureds” or claimants. All “defense costs” and “damages” paid under the Personal CyberPlus® Privacy and Security Claims Coverage Limit of Insurance will reduce, and may completely exhaust, the Combined Aggregate Limit shown in the Schedule.

3. Combined Aggregate Limit

The Combined Aggregate Limit shown in the Schedule is the most “we” will pay under this Coverage Part for all “first party loss” under the Personal CyberPlus® First Party Loss Coverage and all “defense costs” and “damages” under the Personal CyberPlus® Privacy and Security Claims Coverage. If the Combined Aggregate Limit is paid, “our” obligations under this Coverage Part will end.

4. Related Claims

- a. All “first party loss” resulting from the same “insured event”, or a series of related, continuing or repeated “insured events”, will be considered one “insured event”, even if the series of “insured events” continue into a subsequent “policy period”. Such “insured event” will be deemed to have been discovered by “you” on the date the first “insured event” in that series was first discovered by “you” and will be deemed to have been reported to “us” on the date the first “insured event” in that series was reported to “us”.
- b. All “privacy and security claims” arising from the same event, incident, act or circumstance, or a series of related, repeated or continuing events, incidents, acts or circumstances, will be deemed to be a single “privacy and security claim”; will be deemed to have been first made against “you” on the date the earliest of such “privacy and security claims” was first made against “you”; and will be deemed to have been first reported to “us” on the date the earliest of such “privacy and security claims” was first reported to “us” in writing. Appeals and any post-trial proceedings or consolidated proceedings will be part of the original “privacy and security claim”.
- c. If a “privacy breach” or “security breach” reported to “us” under the Personal CyberPlus® First Party Loss Coverage results in a “privacy and security claim” under the Personal CyberPlus® Privacy and Security Claims Coverage, such matters will be deemed to be related, even if the “privacy and security claim” is made against “you” in a subsequent “policy period”. Such “privacy and security claim” will be subject to the Limits of Insurance of the “policy period” in effect when the “privacy breach” or “security breach” was first discovered by an “insured”.

SECTION III. – CONDITIONS

1. Other Insurance

a. Primary Insurance

The coverage provided by this Coverage Part is primary to any other valid and collectible insurance available to “you” under any other insuring agreement or coverage section of the Policy to which this Coverage Part attaches.

b. Excess Insurance

The coverage provided by this Coverage Part is excess insurance over any other valid and collectible insurance available to “you” under any other policy, including any self-insured retention or deductible portion thereof, unless such insurance specifically applies as excess insurance over the insurance provided under this Coverage Part.

2. Your Duties in the Event of a Privacy and Security Claim or Insured Event

- a. “You” must notify us of an “insured event” or “privacy and security claim” as soon as practicable during the “policy period”, but no later than 60 days after expiration or termination of the “policy period”.
- b. “You” must immediately send us copies of any demands, notices, summonses or legal papers that “you” receive in a connection with a “privacy and security claim”.
- c. “You” must submit to “us” any supporting receipts, bills, records or other documents within 90 days of “our” request. “We” may also request a signed and notarized description of any “privacy and security claim” or “insured event” or proof of “first party loss”.
- d. “You” must cooperate with “us” fully and authorize “us” to obtain records and other information.
- e. “You” must assist “us”, upon “our” request, in the enforcement of any right against any person or organization which may be liable to “you” because of “first party loss”, “defense costs” or “damages” to which this insurance applies.

3. Due Diligence

All “insureds” agree to use due diligence to prevent and mitigate “first party loss”, “defense costs” or “damages” covered under this Coverage Part. 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 Coverage Part does not represent advice or counsel from “us” about what “you” should or should not do in response to an “insured event” or “privacy and security claim”.

5. Bankruptcy

“Your” bankruptcy or insolvency will not relieve “us” of “our” obligations under this Coverage Part.

6. Office of Foreign Assets Control

Payment under this Coverage Part shall only be made in full compliance with all United States of America economic or trade sanctions, laws or regulations, including, but not limited to, sanctions, laws and regulations administered and enforced by the U.S. Treasury Department’s Office of Foreign Assets Control (“OFAC”).

7. Currency, Payments and Cryptocurrency Reimbursement

- a. All premium and losses under this Coverage Part shall be payable in United States dollars.
- b. Adjustment of the value of “cryptocurrency” shall be calculated as of the time the “cryptocurrency crime event” occurred, up to the applicable Limit of Insurance.

8. Assistance and Cooperation

As a condition precedent to coverage under this Coverage Part, every “insured” shall cooperate with “us” and “our” representatives and, upon “our” request, shall submit to examination by “our” representative, under oath if required. Every “insured” shall further cooperate with “us” to do whatever is necessary to secure and effect any rights of indemnity, contribution or apportionment that any “insured” may have. No “insured” shall take any action which in any way increases “our” exposure under this Coverage Part.

9. Subrogation

In the event of any payment under this Coverage Part, the “insured” agrees to give “us” the right to any subrogation and recovery to the extent of “our” payments. The “insured” agrees to execute all papers required and do everything that is reasonably necessary to secure these rights to enable “us” to bring an action in the “insured’s” name. The “insured” agrees to fully cooperate in “our” prosecution of that action. The “insured” agrees not to take any action that could impair “our” right of subrogation without “our” express written consent, whether or not the “insured” has incurred any unreimbursed payment. Any recoveries shall be applied first to subrogation expenses, second to amounts paid by “us” under this Coverage Part, and lastly to any applicable deductible. Any additional amounts recovered shall be paid to the “insured”.

10. Dispute Resolution

a. Mediation

Notwithstanding any other provision of this Coverage Part or the Policy, if any irreconcilable dispute arises between any “insured” and “us” concerning this Coverage Part or coverage for any “insured event” or “privacy and security claim”, the “named insured” and “we” agree that such dispute will be referred to a qualified mediator in a good faith effort to negotiate a resolution of the dispute prior to the initiation of any arbitration or other proceedings. The party invoking the agreement to mediate will provide written notice to the other party setting forth its request to mediate and a brief statement regarding the issue to be mediated. The “named insured” is authorized and directed to accept the Notice of Mediation on behalf of any “insured”.

b. Arbitration

As a condition precedent to any right of action hereunder, in the event that a good faith effort to mediate pursuant to paragraph 10.a. above does not resolve a dispute between any “insured” and “us” concerning this Coverage Part or coverage for any “insured event” or “privacy and security claim”, the “named insured” and “we” agree that such dispute will be determined by final and binding arbitration before a single arbitrator. If the parties cannot mutually select the arbitrator, the parties will refer the selection of the arbitrator to the American Arbitration Association.

11. Cancellation and Non-Renewal

This Coverage Part may not be cancelled separately from the Policy. However, the “named insured” may elect to non-renew this Coverage Part at expiration of the “policy period”. There is no extended reporting period available for this Coverage Part.

SECTION IV. – DEFINITIONS

With respect to the coverage provided by this Coverage Part, certain words are shown in quotations and are defined as follows, whether expressed in singular or plural form.

1. “Act of cyber terrorism” means the premeditated use of disruptive activities, or the threat to use disruptive activities, against a “connected device”, including any associated network and data stored thereon, with the intention to cause harm, to further social, ideological, religious, political, or similar objectives, or to intimidate any person in furtherance of such objectives.
2. “Application program” means any “connected device” software program that performs a particular function or task within the “connected device operating system” for the end-user, including, but not limited to, database programs, web browsers, enterprise software, word processors, graphics software and media players.
3. “Attack vector” means the method or combination of methods that are used in a “hacking attack”.
4. “Attorney” means any person who is duly licensed to practice law at the time and place the legal services are rendered. “Attorney” does not include any “insured”.
5. “Breach notification costs” means:
 - a. reasonable and necessary fees and costs to retain the services of an “attorney” to determine the scope, cause and extent of an actual or suspected “privacy breach” or “security breach”; to determine whether “you” have a legal obligation to provide notification of an actual or suspected “privacy breach” or “security breach” to affected individuals; and/or to assist “you” in notifying affected individuals of a “privacy breach” or “security breach”;
 - b. reasonable and necessary fees and costs to retain the services of an IT forensic investigation firm or IT security expert to investigate and identify the source and scope of a “privacy breach” or “security breach”;
 - c. reasonable and necessary printing costs and mailing and postage expenses to notify affected individuals of a “privacy breach” or “security breach”; and
 - d. reasonable and necessary expenses to provide support activity to individuals affected by a “privacy breach” or “security breach”, including the cost to provide a maximum of 24 months of credit, identity or healthcare record monitoring services, fraud alert services, and credit or identity repair and restoration services.

6. "Business" means any employment, trade, occupation, profession or enterprise intended to realize a benefit or financial gain, whether engaged in on a full-time, part-time, occasional or temporary basis.
7. "Business identity theft" means the theft or unauthorized, unlawful or fraudulent use, access or transfer of a means of identifying a "business", with the intent to commit a crime, or aid or abet another to commit a crime, including the theft or fraudulent use of a "business" name, federal or state tax identification number, or other "business" records or information to establish corporate credit accounts, secure loans or enter into contracts.
8. "Connected device" means any electronic device or appliance, including, but not limited to, any computer, laptop, mobile device, appliance, thermostat, entertainment system, camera, or home security, smoke or fire monitoring system that can send and receive data and is connected to the internet (also known as smart devices). "Connected device" does not include any motor vehicle, watercraft, aircraft or other vehicle.
9. "Connected device operating system" means "connected device" software that manages or administers hardware, software resources, or provides common services to run an "application program". "Connected device operating system" does not include an "application program".
10. "Covered bank account" means a personal account at a financial or banking institution, including any personal trust or investment account, which is maintained by "you" in "your" name, or in the name of a legal entity established by "you" or on "your" behalf to manage "your" personal assets, from which "you" may request the transfer, payment or delivery of "money" or "securities". "Covered bank account" does not include any commercial or non-consumer account or any "cryptocurrency" account.
11. "Covered device" means any "connected device" that is owned or leased, and operated, by "you".
12. "Credit card fraud" means the loss, theft, or unauthorized and fraudulent use of "your" credit, debit or bank card by a person other than "you". "Credit card fraud" does not include the use of "your" credit, debit or bank card by a "family member" without "your" permission.
13. "Criminal proceedings" means any governmental action, indictment or investigation for the enforcement of criminal laws, including offenses for which conviction could result in imprisonment and/or criminal fine(s).
14. "Cryptocurrency" means a medium of exchange that:
 - a. is digital and decentralized;
 - b. uses blockchain to manage and record transactions; and
 - c. is stored by a "cryptocurrency exchange"."Cryptocurrency" includes, but is not limited to, Bitcoin and Ethereum. "Cryptocurrency" does not include "money" or "securities".
15. "Cryptocurrency crime event" means "your" loss of "cryptocurrency" which is fraudulently taken from "you" as a direct result of a "hacking attack".
16. "Cryptocurrency exchange" means an online "business" domiciled in the United States of America that provides a virtual platform to buy, sell, trade and store "cryptocurrency".
17. "Cyber bullying" means a series of two or more willful and repeated or continuing acts of harassment or intimidation, including embarrassment, humiliation, defamation of character, slander, invasion of privacy or threats of violence, committed using a computer, telephone, mobile device or other electronic device. "Cyber bullying" methods include, but are not limited to, the use of texting, instant messaging, chat rooms, and messages, photos and other content posted on social networking sites with the intent to harass and intimidate.
18. "Cyber bullying expenses" means any of the following directly resulting from a "cyber bullying incident":
 - a. reasonable and necessary costs to retain the services of a "therapist" to diagnose and treat the mental anguish or injury caused by a "cyber bullying incident", provided such "therapist" is retained by a "victim" within 12 months after the "cyber bullying incident" is discovered;
 - b. lost salary or wages due to a "victim" being unable to work during the first 120 days after the "cyber bullying incident" is discovered;
 - c. reasonable and necessary childcare or caregiver expenses, provided such services are retained by a "victim" within 120 days after the "cyber bullying incident" is discovered;
 - d. reasonable and necessary expenses to temporarily relocate a "victim", provided such relocation occurs within 120 days after the "cyber bullying incident" is discovered;

- e. if the “victim” is a “minor”, reasonable and necessary temporary private tutoring expenses due to the “victim” being unable to attend school, provided such tutoring services are retained within 120 days after the “cyber bullying incident” is discovered;
 - f. if the “victim” is a “minor”, unreimbursed tuition, new school enrollment fees and increase in tuition to transfer the “minor” to another school, provided such transfer occurs within 120 days after the “cyber bullying incident” is discovered;
 - g. reasonable and necessary fees and costs to retain a digital forensic analyst or professional cyber security consultant, provided such services are retained by a “victim” within 12 months after the “cyber bullying incident” is discovered; and
 - h. “internet clean-up costs”.
19. “Cyber bullying incident” means “cyber bullying” directed at “you”, which causes “you” to suffer mental anguish or mental injury, as diagnosed by a “therapist”.
20. “Cyber crime event” means:
- a. “wire transfer fraud”;
 - b. a “phishing attack” directed at “you”, which fraudulently induces “you” to willingly transfer, pay or deliver “money” or “securities” to an unintended party through a traceable means of delivery, including, but not limited to, check, wire transfer or credit or debit card payment; however, cash is not a traceable method of delivery; or
 - c. the theft of “money” or “securities” from a “covered bank account” as a result of a “hacking attack”.
21. “Cyber extortion expenses” means reasonable and necessary costs and expenses, other than “cyber extortion monies”, that directly result from a “cyber extortion threat”, including the cost to retain or hire a “third party” specializing in IT security to determine the validity and severity of a “cyber extortion threat” and/or provide advice regarding how best to respond to a “cyber extortion threat”.
22. “Cyber extortion monies” means “money” or “cryptocurrency” that “you” pay to a person or group reasonably believed to be responsible for a “cyber extortion threat” in order to prevent or terminate such “cyber extortion threat”.
23. “Cyber extortion threat” means a credible threat, or a series of related credible threats, made by a “third party”, including a demand for “cyber extortion monies”, which is directed at “you” to:
- a. steal, alter, release, reveal, divulge, disseminate, destroy, publicly disclose or misuse “private information” contained in a “covered device”;
 - b. infect a “covered device” with a “virus”;
 - c. corrupt, damage, disable, destroy or alter a “covered device”; or
 - d. deny, restrict or hinder access to a “covered device”, including the threat of a “denial of service attack”.
24. “Cyber operation” means the use of a “connected device” by, at the direction, or under the control of a sovereign state to disrupt, deny, degrade, manipulate or destroy information in a “connected device” or in another sovereign state.
25. “Damages” means a monetary judgment, award or settlement that an “insured” is legally obligated to pay because of a “privacy and security claim”. “Damages” does not include punitive, liquidated, exemplary or multiplied damages; fines, penalties, taxes or sanctions; the costs to comply with any judgment, award, court order or settlement; liability assumed under a contract; any amount which an “insured” is not financially or legally obligated to pay; or any amounts deemed uninsurable under applicable law.
26. “Data recovery expenses” means the costs to retain a data recovery service provider to retrieve, replace or restore “your” electronic data that has been lost, damaged or corrupted in a “hacking attack”. If it is determined that “your” data cannot be retrieved, replaced or restored, “we” will reimburse only the actual and necessary “data recovery expenses” incurred up to the date of such determination. “Data recovery expenses” does not include costs to research, recreate or replace software programs or operating systems that are obsolete or not commercially available, or data that cannot reasonably be replaced, including, but not limited to, photographs, music, movies or other media or recordings for which no back-up is available.
27. “Defense costs” means reasonable and necessary fees for legal services rendered by an “attorney”, and associated costs and expenses, incurred by “you” in the defense of a “privacy and security claim”.
28. “Denial of service attack” means an event caused by unauthorized or unexpected interference or a malicious attack, which is intended by the perpetrator to overwhelm the capacity of a “connected device” by sending an excessive volume of data to such “connected device” to deny, restrict or hinder access to such “connected device”.

- 29.** “Domestic partner” means any person qualifying as such under the provisions of any applicable federal, state or local law.
- 30.** “Essential service” means any service that is essential for the proper operation and maintenance of vital functions of a sovereign state, including, but not limited to, financial services (including services related to financial institutions and associated financial market infrastructure), health services, utility services, emergency services, and/or services that are essential for the proper operation of the food, energy and/or transportation sector.
- 31.** “Family member” means any of the following persons residing with the “named insured”:
- a.** the spouse or “domestic partner” of the “named insured”;
 - b.** any “minor”;
 - c.** a student enrolled in school full time, as defined by the school, who was a member of the “named insured’s” household before moving out to attend school, provided the student is under the age of 24 and related to the “named insured” by blood, marriage or adoption; and
 - d.** other persons related to the “named insured” by blood, marriage or adoption.
- 32.** “Financial fraud loss” means “your” loss of “money” or “securities” which is fraudulently taken from “you” as a direct result of a “cyber crime event”.
- 33.** “First party loss” means:
- a.** solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement **1.a.**, “identity theft expenses”;
 - b.** solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement **1.b.**, “data recovery expenses” and “system restoration costs”;
 - c.** solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement **1.c.**, “your” loss of “money” as a direct result of “credit card fraud” or “forgery”;
 - d.** solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement **1.d.**, “financial fraud loss”;
 - e.** solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement **1.e.**, “your” loss of “cryptocurrency” as a direct result of a “cryptocurrency crime event”;
 - f.** solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement **1.f.**, “cyber extortion expenses” and “cyber extortion monies”;
 - g.** solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement **1.g.**, “cyber bullying expenses”; and
 - h.** solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement **1.h.**, “breach notification costs”.
- 34.** “Forgery” means the alteration of “your” negotiable instrument, or the imitation of “you” on a negotiable instrument, with instructions to pay, including counterfeit items, and with the intent to deceive.
- 35.** “Hacking attack” means a malicious or unauthorized electronic attack that is initiated by a “third party”, directed at or enacted upon a “covered device”, and designed to damage, destroy, corrupt, overload or impair the functionality of the “covered device”, including:
- a.** unauthorized access to, or unauthorized use of, the “covered device”, including any such unauthorized access or unauthorized use resulting from the theft of a password from the “covered device” or from an “insured”;
 - b.** a “denial of service attack”; or
 - c.** infection of the “covered device” with a “virus”.
- 36.** “Identity theft” means the act of knowingly transferring or using, without lawful authority, a means of “your” personal identification, with the intent to commit a crime, or aid or abet another to commit a crime, including the fraudulent use of “your” personal identity to establish credit accounts, secure loans or enter into contracts. “Identity theft” includes the fraudulent use of “your” health insurance numbers to file false health insurance claims or to seek medical treatment or prescription drugs, but does not include “business” “identity theft”.
- 37.** “Identity theft expenses” means any of the following directly resulting from “identity theft”:
- a.** reasonable and customary notary and certified mail charges for completing and delivering fraud affidavits to law enforcement agencies, credit agencies, health insurance companies, or financial institutions or similar credit grantors;

- b. reasonable and customary application fees to reapply for a loan, grant or other credit instrument that was denied or rejected solely because the original application contained inaccurate information due to “identity theft”;
 - c. “your” employer-documented lost wages or salaried earnings from time taken off work to meet with an “attorney” or law enforcement agencies, credit agencies, health insurance companies, healthcare providers, merchants, or financial institutions or similar credit grantors to complete fraud affidavits, restore “your” identity or credit history, or otherwise resolve the “identity theft”, up to a maximum payment of \$200 per day and \$5,000 in the aggregate for any one “policy period”, regardless of the number of impacted “insureds”;
 - d. “your” reasonable daycare or eldercare costs, if daycare or eldercare is necessary for “you” to meet with an “attorney” or law enforcement agencies, credit agencies, health insurance companies, healthcare providers, merchants, or financial institutions or similar credit grantors to complete fraud affidavits, restore “your” identity or credit history, or otherwise resolve the “identity theft”, up to a maximum of \$1,000 per week for up to 5 weeks; provided, however, that such daycare or eldercare must be provided by a professional care provider who is not a “family member”;
 - e. “your” reasonable and necessary travel and accommodations expenses to resolve “identity theft”, up to a maximum limit of \$1,000 per week for up to 5 weeks;
 - f. long distance telephone charges or cellular phone charges for calls to an “attorney” or law enforcement agencies, credit agencies, health insurance companies, healthcare providers, merchants, financial institutions or similar credit grantors to report or discuss “identity theft”;
 - g. reasonable and necessary “attorney” fees and associated costs to:
 - (1) defend lawsuits brought against “you” by merchants, financial institutions or their collection agencies;
 - (2) remove criminal or civil judgments wrongly entered against “you” as a result of “identity theft”;
 - (3) challenge the accuracy or completeness of information in a consumer credit report;
 - (4) release medical records in cases of medical identity fraud;
 - (5) contest a tax liability wrongfully incurred by “you” as a result of “identity theft”;
 - (6) contest the wrongful transfer of ownership of “your” tangible property; or
 - (7) provide “you” with assistance or representation at an audit or hearing before a government agency;
 - h. reasonable and customary fees for the reapplication and reissuance of government-issued identification documentation, such as passports, driver’s licenses, personal identification cards or social security cards, if compromised because of “identity theft”;
 - i. reasonable and customary fees for copies of medical records solely to investigate medical identity fraud, upon exhaustion of a healthcare provider’s medical record request and appeal process;
 - j. reasonable and customary costs to obtain “your” credit reports from established credit bureaus; such credit reports must be dated within 12 months after “you” first discover the “identity theft”, and no more than two credit reports may be obtained from any one established credit bureau; and
 - k. reasonable and customary costs to monitor “your” credit for up to 24 months; such credit monitoring must begin no later than 6 months after “you” first discover the “identity theft”.
- 38. “Impacted state” means a sovereign state where a “cyber operation” has had a major detrimental impact on:**
- a. the functioning of that sovereign state due to disruption of the availability, integrity or delivery of an “essential service” in that sovereign state; and/or
 - b. the security or defense of that sovereign state.
- 39. “Insured” means the “named insured” and any “family member”.**
- 40. “Insured event” means:**
- a. solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement **1.a.**, “identity theft”;
 - b. solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement **1.b.**, a “hacking attack”;
 - c. solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement **1.c.**, “credit card fraud” or “forgery”;
 - d. solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement **1.d.**, a “cyber crime event”;

- e. solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement 1.e., a “cryptocurrency crime event”;
 - f. solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement 1.f., a “cyber extortion threat”;
 - g. solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement 1.g., a “cyber bullying incident”; and
 - h. solely with respect to Personal CyberPlus® First Party Loss Coverage, Insuring Agreement 1.h., a “security breach” or “privacy breach”.
41. “Internet clean-up costs” means reasonable and necessary fees and costs to retain an “attorney”, digital forensic analyst or professional cyber security consultant to remove content posted on the internet by the perpetrator of a “cyber bullying incident”.
42. “Minor” means any person under 21 years of age who is residing with the “named insured” and is related to the “named insured” by blood, marriage, adoption or legal guardianship.
43. “Money” means a medium of exchange in current use and authorized or adopted by a domestic or foreign government, including, but not limited to, currency, coins, bank notes, bullion, travelers’ checks, registered checks and “money” orders held for sale to the public. “Money” does not include “cryptocurrency” or “securities”.
44. “Named insured” means any natural person listed as such on the Policy declaration page.
45. “Operating system event” means a single act of exploitation of, or a series of related, repeated or continuing acts of exploitation of, software vulnerabilities in a “connected device operating system”, including, but not limited to ransomware, wiper malware, computer worms, and “viruses”, the impact of which is of sufficient intensity, scale or effect to cause a major detrimental impact on the functioning of a sovereign state due to disruption of the availability, delivery, or integrity of any “essential service” in that sovereign state; provided, however, a major detrimental impact on the functioning of a sovereign state shall not result from an attack, or a related series of attacks, solely impacting “you”. For purposes of this definition, the determination of whether an event constitutes a major detrimental impact on the functioning of a sovereign state will rely upon any available evidence such as information from governments, news media, qualified IT forensics firms, computer experts and claims reported to “us”.
46. “Other property” means any tangible property, other than “money” or “securities”, which has intrinsic value.
47. “Personally identifiable information” means information that can be used to determine, distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, including, but not limited to, financial account numbers, security codes, personal identification numbers (PINs), credit and debit card numbers, medical or healthcare information, social security numbers, driver’s license numbers, addresses, passwords, and any other non-public information.
48. “Phishing attack” means the use by a “third party” of fraudulent and intentionally deceptive telephone calls, emails, texts, instant messages or other electronic communications or malicious websites to impersonate a legitimate or trustworthy contact, organization or person to solicit “private information”, “money” or “securities”.
49. “Policy period” means the period of time from the effective date to the expiration date specified in the Declarations of the Policy, or any earlier cancellation or termination date; provided, however, that the “policy period” shall not exceed a period of 12 months.
50. “Privacy and security claim” means a “suit” alleging:
- a. liability for a “privacy breach”;
 - b. liability for the failure to prevent the transmission of a “virus” from a “covered device” to a “connected device” of a “third party”;
 - c. liability for the failure to prevent or hinder participation by a “covered device” in a “denial of service attack” directed against a “connected device” of a “third party”;
 - d. liability for “cyber bullying” committed by a “minor” or by a person posing as “you”;
 - e. liability for the failure to prevent or hinder a “security breach”, which in turn results in a “privacy breach”;
 - f. liability for the failure to timely disclose a “security breach” or “privacy breach” affecting “private information”; or
 - g. infliction of emotional distress or mental anguish, but only if directly resulting from a peril described in paragraphs a. through f. above.

A “privacy and security claim” will be deemed to be first made against “you” when it is first received by “you”.

51. "Privacy breach" means:

- a.** the unauthorized collection, disclosure, use, access, destruction or modification of "private information";
- b.** the theft of "private information", including the theft of "private information" stored on a "covered device";
- c.** "your" surrender of "private information" in a "phishing attack"; or
- d.** an infringement or violation of any rights to privacy directly resulting from a peril described in paragraphs **a.** through **c.** above.

52. "Private information" means "personally identifiable information" of a "third party" that is in "your" possession or entrusted to "you" solely because of "your" activities or responsibilities in connection with volunteer work for a non-profit organization or other non-"business" related activity. "Private information" does not include any "business" records or information, including proprietary information.

53. "Private key" means a string of letters and/or numbers that are used to access and manage "cryptocurrency" and/or secure and verify "cryptocurrency" transactions.

54. "Related hacking attack" means a "hacking attack" with:

- a.** the same actor or a coordinated group of actors;
- b.** the same "attack vector";
- c.** the same vulnerability; or
- d.** the common impacted vendor or group of impacted vendors as any other person or entity holding cyber insurance coverage through "us".

"Related hacking attack" does not include a "hacking attack" which deceives or manipulates any "insured" to execute subsequent, intervening actions in order to constitute or cause the "privacy and security claim" or "insured event".

55. "Securities" means negotiable or non-negotiable instruments or contracts representing "money" or "other property". "Securities" does not include "money" or "cryptocurrency".

56. "Security breach" means any of the following, whether a specifically targeted attack or a generally distributed attack:

- a.** a "hacking attack"; or
- b.** the theft or loss of a "covered device" containing "private information".

57. "Suit" means:

- a.** the service of a civil lawsuit or the institution of arbitration or other alternative dispute resolution proceedings against "you" seeking "damages" or non-monetary relief; or
- b.** a written demand made against "you" for "damages" or non-monetary relief.

58. "System restoration costs" means reasonable and necessary costs to retain a qualified service provider to restore a "covered device" to the same level of functionality that existed prior to a "hacking attack", including services such as replacing or reinstalling computer software programs, removing a "virus", and configuring or correcting the configuration of the "covered device".

"System restoration costs" does not include:

- a.** any costs to upgrade or increase the speed, capacity or utility of the "covered device" to a level that exceeds that which existed prior to the "hacking attack";
- b.** any costs that exceed the actual cash value of the "covered device"; or
- c.** "your" time or labor.

59. "Therapist" means a qualified psychologist or other mental health professional who is licensed and/or certified under the laws of the jurisdiction in which mental health treatment is given to "you" as a "victim" of a "cyber bullying incident". "Therapist" does not include any "insured".

60. "Third party" means any entity, company, organization or person who does not qualify as an "insured" under this Coverage Part.

61. "Unauthorized trading" means trading, which at the time of the trade, exceeds permitted financial limits or is outside of permitted product lines.

62. "Victim" means any "insured" who suffers mental anguish or mental injury as a direct result of a "cyber bullying incident".

63. "Virus" means malicious software intentionally designed to insert itself by a variety of forms into a "connected device" to damage, destroy, corrupt, overload or otherwise impair the functionality of such "connected device". "Virus" includes, but is not limited to, worms, Trojan horses, spyware, dishonest adware and malware.
64. "War" means any war, invasion, acts of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power, or confiscation, nationalization, requisition or destruction of or damage to property by or under the order of any government or public or local authority, or any action taken by a government authority to hinder, control, prevent, suppress or defend against any of the aforementioned actions.
65. "We", "us" and "our" mean the Company providing the insurance under this Coverage Part.
66. "Widespread event" means an "act of cyber terrorism" or a "related hacking attack" that impacts 200 other persons or entities holding cyber insurance coverage through "us" that is discovered, or should have been discovered, within 90 days of the first such person or entity discovering, or when the first such person or entity should have discovered, such "act of cyber terrorism" or "hacking attack".
67. "Wire transfer fraud" means an intentional, unauthorized and fraudulent written, electronic or telephonic instruction transmitted to a financial institution, directing such institution to debit, transfer, withdraw or disburse "money" or "securities" from a "covered bank account", which instruction purports to have been transmitted by "you", but was in fact fraudulently transmitted by a "third party" without "your" knowledge or consent. "Wire transfer fraud" does not include fraud committed against any "business", commercial or non-consumer account or any "cryptocurrency" account.
68. "You" and "Your" mean any "insured".

SECTION V. – ENTIRE AGREEMENT

By acceptance of this Coverage Part, the "named insured" agrees that this Coverage Part embodies all agreements between the "named insured" and "us" relating to this Coverage Part. Notice to any agent, or knowledge possessed by any agent or any other person, will not affect a waiver or change in this Coverage Part, or estop "us" from asserting any right under the terms of this Coverage Part; nor will the terms of this Coverage Part be waived or changed, except by endorsement issued to form a part of this Coverage Part and signed by "us".