

PLEASE READ THIS ENTIRE FORM CAREFULLY.

FARM CYBERPLUS™ COVERAGE PART

SCHEDULE

	Limit of Insurance
First Party Loss Coverage: (Event discovered and reported coverage)	\$
Third Party Claims Coverage: (Claims-made and reported coverage)	\$
Bodily Injury or Property Damage Claims Sublimit: (Sublimit of the Third Party Claims Coverage)	\$
Combined Aggregate Limit:	\$

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

THE LIMITS OF INSURANCE SHOWN IN THE SCHEDULE ABOVE WILL BE REDUCED AND MAY BE COMPLETELY EXHAUSTED BY ALL AMOUNTS PAID UNDER THIS COVERAGE PART, INCLUDING LEGAL EXPENSES.

INSURING AGREEMENT

"We" will provide insurance described in this Coverage Part in compliance with all applicable provisions, including but not limited to, 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, to which this Coverage Part is attached to.

SECTION I – FIRST PARTY LOSS COVERAGE AND EXCLUSIONS

The following coverages are subject to the First Party Loss Coverage Limit of Insurance.

1. Identity Theft Expense Coverage

"We" will pay for "identity theft expenses" that an "insured" incurs solely and directly because of "identity theft", provided that the "identity theft":

- a. Is discovered during the "policy period"; and
- b. Is reported 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. System Failure (Data Recovery and Non-Physical Farming Interruption) Coverage

a. Data Recovery

Subject to a \$500 deductible, "we" will pay "digital assets loss" and "special expenses" that an "insured" incurs solely and directly because of damage, alteration, corruption, distortion, theft, misuse or destruction of "digital assets" resulting from a "system failure", provided that the "system failure":

- (1) Is discovered during the "policy period"; and

- (2) Is reported 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) The “insured” provides clear evidence that the “digital assets loss” and “special expenses” directly resulted from the “system failure”.

“We” will pay “digital assets loss” and “special expenses” for up to 12 months following discovery of the “system failure” by an “insured”.

The \$500 deductible applies to any one “system failure”. If the amount of “digital assets loss” and/or “special expenses” resulting from any one “system failure” is less than or equal to the deductible, “we” will not pay for those “digital assets loss” and/or “special expenses”. If the amount of “digital assets loss” and/or “special expenses” resulting from any one “system failure” exceeds the deductible, “we” will subtract the deductible from the amount of “digital assets loss” and/or “special expenses” incurred, and “we” will pay the remaining amount of “digital assets loss” and/or “special expenses”, up to the applicable Limit of Insurance.

b. Non-Physical Farming Interruption

Subject to the applicable “waiting period”, “we” will pay “income loss”, “interruption expenses” and “special expenses” that “you” incur during the “period of restoration” solely and directly because of a “system failure”, provided that the “system failure”:

- (1) Is discovered during the “policy period”; and
- (2) Is reported to “us” 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 “income loss”, “interruption expenses” and “special expenses” directly resulted from the “system failure”.

3. Credit Card Fraud & Forgery Coverage

“We” will pay for the loss of “money” that the “insured” incurs solely and directly because of “credit card fraud” or “forgery”, provided that the “credit card fraud” or “forgery”:

- a. Is discovered during the “policy period”; and
- b. Is reported 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
- c. The “insured” notifies the “insured’s” credit card company or bank of the facts and circumstances surrounding the “credit card fraud” or “forgery” as soon as practicable; and
- d. The “insured” provides written confirmation to “us” that the “insured’s” credit card company or bank has refused to reverse or prevent a payment transaction, or to indemnify or reimburse the “insured” for the loss of “money”.

4. Cyber Crime Coverage

“We” will pay for “financial fraud loss” that the “insured” incurs solely and directly because of a “cyber crime event”, provided that the “cyber crime event”:

- a. Is discovered during the “policy period”; and
- b. Is reported 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
- c. The “insured” provides written confirmation to “us” that the “insured’s” bank has refused to reverse or prevent a payment transaction, or to indemnify or reimburse the “insured” for the “financial fraud loss”.

5. Cryptocurrency Crime Coverage

“We” will pay for the loss of “cryptocurrency” that the “insured” incurs solely and directly because of a “cryptocurrency crime event”, provided that the “cryptocurrency crime event”:

- a. Is discovered during the “policy period”; and
- b. Is reported 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
- c. The “insured” provides written confirmation to “us” that the “insured’s” “cryptocurrency exchange” has refused to reverse or prevent a payment transaction, or to indemnify or reimburse the “insured” for the loss of “cryptocurrency”.

6. Cyber Extortion Coverage

"We" will pay for "cyber extortion expenses" and "cyber extortion monies" that the "insured" incurs solely and directly because of a "cyber extortion threat", provided that the "cyber extortion threat":

- a. Is discovered during the "policy period"; and
- b. Is reported 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".

7. Cyber Bullying Coverage

"We" will pay for "cyber bullying expenses" that the "insured" incurs solely and directly because of a "cyber bullying incident", provided that the "cyber bullying incident":

- a. Is discovered during the "policy period"; and
- b. Is reported 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".

8. Breach Notification Coverage

"We" will pay for "privacy breach response costs" that "you" incur and for "notification expenses" and "breach support and credit monitoring expenses" that the "insured" incurs solely and directly because of an "adverse media report", "security breach" or "privacy breach", provided that the "adverse media report", "security breach" or "privacy breach":

- a. Is discovered during the "policy period"; and
- b. Is reported 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".

9. BrandGuard® Coverage

Subject to the applicable "waiting period", "we" will pay provable and ascertainable "brand loss" that "you" sustain during the "period of indemnity" solely and directly because of an "adverse media report" or "notification" of a "security breach" or "privacy breach", provided that the "security breach" or "privacy breach":

- a. Is discovered during the "policy period"; and
- b. Is reported to "us" during the "policy period", but no later than 60 days after the expiration or termination of the "policy period"; and
- c. "You" provide clear evidence that the "brand loss" is directly attributable to the "adverse media report" or "notification".

EXCLUSIONS APPLICABLE TO FIRST PARTY LOSS COVERAGE

The following exclusions apply to all First Party Loss Coverages.

"We" do not cover:

1. Any amounts incurred by an "insured" in disputes with respect to this insurance, including questions as to whether amounts are payable under this Coverage Part.
2. Any costs to replace or repair any property, hardware or "insured computer system".
3. Any amounts incurred by an "insured" to institute legal proceedings against a person or organization.
4. Any "loss" incurred by "your" former spouse or "domestic partner", or a "family member" who is no longer residing with "you".
5. "Loss" arising from:
 - a. A false report of an "insured event" made by an "insured", whether acting alone or in collusion with others.
 - b. Any willful, intentional, malicious or criminal acts committed by an "insured" or any person residing with "you"; 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.
 - c. Fire, smoke, explosion, leakage, lightning, wind, water, flood (including waves, tidal waves, or the rising of, breaking out of, or overflow of a body of water, whether natural or manmade), earthquake, volcanic eruption, landslide, hail, extreme weather, or any other natural event.
 - d. The seizure, confiscation, nationalization, requisition or destruction of any "insured computer system", "data", hardware or equipment by or under order of any government or public authority.

6. Any “insured event” which was known to any “insured” prior to the effective date of this Coverage Part.
7. “Property damage” or “bodily injury”.
8. Liability assumed by an “insured” under a written or oral contract or agreement.
9. Any activities of, or relating to, a “business” owned or operated by any “insured”.
10. The failure of overhead transmission and distribution lines.
11. Any regional, countrywide or global 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.
12. Any costs to comply with any order, grant or agreement to provide non-monetary relief.
13. Any “business” use of a credit, debit or bank card.
14. “Business identity theft”.
15. A total, partial, temporary or intermittent outage of internet connection.
16. Fines, penalties, taxes or sanctions imposed by law, or any matters deemed uninsurable under applicable law.
17. Any amounts an “insured” is legally obligated to pay to a “third party”, including judgments, awards or settlements.
18. “Criminal proceedings”; however, this exclusion does not apply to “identity theft expenses” incurred to remove criminal judgments wrongly entered against an “insured” as a result of “identity theft”.
19. Any amounts paid or payable under the Third Party Claims Coverage.
20. Any matter other than an “insured event”.
21. Loss of “cryptocurrency” arising from:
 - a. An outage, interruption, failure, suspension or degradation of service of a “computer system” owned, controlled, leased or operated by a “cryptocurrency exchange”;
 - b. 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
 - c. The insolvency or bankruptcy of any “cryptocurrency exchange”.
22. “Loss” arising 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:
 - a. 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”;
 - b. If an “insured” has not complied with all terms and conditions under which such card, card number or account number was issued; or
 - c. In connection with the operation of any “business”.
23. Any amounts that have been wholly or partially reversed, or reimbursed to an “insured”, by a credit card company, bank or “cryptocurrency exchange”.
24. An “insured’s” loss of “other property” arising out of, resulting from or involving the fraudulent or purportedly fraudulent use of a credit or debit card.
25. “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:
 - a. That are not yet delivered, whether fraudulent or not;
 - b. That fail to conform to advertised quality or performance; or
 - c. That fail to conform to the quality or performance expected from the standpoint of the “insured”.

26. An “insured’s” 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 an “insured”; however, this exclusion does not apply to lost wages directly resulting from “identity theft” or a “cyberbullying incident”.
27. Any “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.
28. “Loss”, cost or expense:
- a. Directly or indirectly caused by, resulting from or in connection with any “war”;
 - b. Resulting from a “cyber operation” carried out as part of any “war”; or
 - c. Resulting from a “cyber operation” that causes a sovereign state to become an “impacted state”.
- However, this exclusion does not apply to an “act of cyber terrorism”. Paragraph c. above shall not apply to the direct or indirect effect of a “cyber operation” on an “insured computer system” that is not physically located in an “impacted state” but is affected by a “cyber operation”.
29. “Loss” arising from a “widespread event”. The determination of what 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”.
30. Any matter paid, or deemed payable, by “us” under any other insuring agreement or coverage part of the Policy.

SECTION II – THIRD PARTY CLAIMS COVERAGE AND EXCLUSIONS

The following coverages are subject to the Third Party Claims Coverage Limit of Insurance

1. Media Liability Coverage

“We” will pay “damages”, including liability “assumed under contract”, and reasonable and necessary “legal expenses” that an “insured” incurs in a “media claim”, provided that the “media claim”:

- a. Is made against the “insured” during the “policy period”; and
- b. Is reported to “us” during the “policy period”, but no later than 60 days after expiration or termination of the “policy period”; and
- c. The actual or alleged “media wrongful act” giving rise to the “media claim” is committed or allegedly committed on or after the inception date of the first Coverage Part issued by “us” to “you”.

2. Privacy and Security Liability Coverage

“We” will pay “damages”, including liability “assumed under contract”, and reasonable and necessary “legal expenses” that an “insured” incurs in a “privacy and security claim”, provided that the “privacy and security claim”:

- a. Is made against the “insured” during the “policy period”; and
- b. Is reported to “us” during the “policy period”, but no later than 60 days after expiration or termination of the “policy period”; and
- c. The actual or alleged “privacy and security wrongful act” giving rise to the “privacy and security claim” is committed or allegedly committed on or after the inception date of the first Farm CyberPlus™ Coverage Part issued by “us” to “you”.

3. Privacy Regulatory Liability Coverage

“We” will pay “regulatory compensatory awards”, “regulatory fines and penalties” and reasonable and necessary “legal expenses” that an “insured” incurs in a “privacy regulatory proceeding”, provided that the “privacy regulatory proceeding”:

- a. Is first instituted against the “insured” during the “policy period”; and
- b. Is reported to “us” during the “policy period”, but no later than 60 days after expiration or termination of the “policy period”; and
- c. The actual or alleged “security breach” or “privacy breach” giving rise to the “privacy regulatory proceeding” first occurs on or after the inception date of the first Farm CyberPlus™ Coverage Part issued by “us” to “you”.

4. PCI DSS Liability Coverage

"We" will pay "PCI DSS fines and assessments" and reasonable and necessary "legal expenses" that an "insured" incurs in a "PCI DSS claim", provided that the "PCI DSS claim":

- a. Is first made against the "insured" during the "policy period"; and
- b. Is reported to "us" during the "policy period", but no later than 60 days after expiration or termination of the "policy period"; and
- c. The actual or alleged "security breach" or "privacy breach" giving rise to the "PCI DSS claim" first occurs on or after the inception date of the first Farm CyberPlus™ Coverage Part issued by "us" to "you".

5. Network Security Bodily Injury and Property Damage Liability Coverage

Subject to the "bodily injury or property damage claims sublimit", "we" will pay "damages" and reasonable and necessary "legal expenses" that an "insured" incurs in a "bodily injury or property damage claim", provided that the "bodily injury or property damage claim":

- a. Is first made against the "insured" during the "policy period"; and
- b. Is reported to "us" during the "policy period", but no later than 60 days after expiration or termination of the "policy period"; and
- c. The actual or alleged "security breach" giving rise to the "bodily injury or property damage claim" first occurs on or after the inception date of the first Farm CyberPlus™ Coverage Part issued by "us" to "you".

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

- a. "We" shall have no duty to defend any "claim" under the Third Party Claims Coverage, but only to pay "legal expenses" and "loss". The obligation to defend any "claim" under the Third Party Claims Coverage resides solely with an "insured", and a reasonable and good faith defense of any "claim" by the "insured" is a condition precedent to coverage under the Third Party Claims Coverage.
- b. An "insured" shall have complete freedom of choice in the selection of an "attorney" to represent the "insured" in any "claim". However, payment for "legal expenses" will be limited to a maximum hourly "attorney" rate of \$400. An "insured" will have a direct relationship with any "attorney" retained by the "insured".
- c. There shall be no infringement upon the professional judgment of any "attorney", and no "attorney" providing legal services in respect of which "legal expenses" are payable under this Coverage Part shall be required to act in derogation of such "attorney's" professional responsibilities.

EXCLUSIONS APPLICABLE TO THIRD PARTY CLAIMS COVERAGE

The following exclusions apply to all Third Party Claims Coverage.

"We" do not cover:

1. Any amounts incurred by an "insured" in disputes with respect to this insurance, including questions as to whether amounts are payable under this Coverage Part.
2. Any amounts incurred by an "insured" to institute legal proceedings against a person or organization.
3. Any "claim" for, based upon, arising from or involving any "wrongful act" which was known to any "insured" prior to the effective date of this Coverage Part.
4. Any matter brought against an "insured" for, based upon, arising from or involving "property damage" or "bodily injury"; however, this exclusion does not apply to any "bodily injury or property damage claim".
5. Any "claim" for, based upon, arising from or involving any liability assumed by an "insured" under a written or oral contract or agreement; however, this exclusion does not apply to:
 - a. A "media claim" or "privacy and security claim" for liability "assumed under contract";
 - b. Any liability an "insured" would have had in the absence of such contract or agreement and which would have been insured under this Coverage Part; or
 - c. With respect to a "PCI DSS claim", liability for "PCI DSS fines and assessments" assumed by "you" under a "merchant services agreement".

6. Any “claim” based upon, arising from or involving any breach of any express, implied, actual or constructive contract, warranty, guarantee or promise; however, this exclusion does not apply to:
- a. Any liability an “insured” would have had in the absence of such contract, warranty, guarantee or promise and which would have been insured under this Coverage Part;
 - b. An actual or alleged breach of “your privacy policy”;
 - c. An actual or alleged breach of an express, implied, actual or constructive contract, warranty, guarantee or promise to protect “private information”;
 - d. A “privacy and security claim” arising out of an “insured’s” unintentional breach of the provisions of a confidentiality or non-disclosure agreement relating to the confidentiality of “private information”; or
 - e. A “PCI DSS claim” arising out of an “insured’s” unintentional breach of the provisions of a “merchant services agreement” relating to compliance with the “PCI Data Security Standard”.
7. Any “claim” based upon, arising from or involving activities of a “business” owned or operated by “you”.
8. Any “claim” for, based upon, arising from or involving any of the following committed by an “insured” whether acting alone or in collusion with other persons:
- a. Any willful, intentional, malicious, fraudulent or criminal act or omission;
 - b. Any intentional violation of law; or
 - c. The gaining of any profit or advantage to which an “insured” is not legally entitled.

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.

9. Any costs to comply with any order, grant or agreement to provide non-monetary relief.
10. Any matter deemed uninsurable under applicable law.
11. Punitive, exemplary, liquidated or multiplied damages.
12. Any “claim” made by or on behalf of an “insured” against another “insured”; however, this exclusion does not apply to a “privacy and security claim” brought against “you” by any “employee” for, based upon or arising from a “privacy breach” of the “personally identifiable information” of such “employee”.
13. “Criminal proceedings”.
14. Any amounts paid or payable under the First Party Loss Coverage.
15. Any matter other than a “claim”.
16. Any matter paid, or deemed payable, by “us” under any other insuring agreement or coverage part of the Policy;
17. Any “claim” based upon, arising from or involving the actual or alleged government enforcement of any foreign, federal, state or local regulation including, but not limited to, regulations promulgated by the United States Federal Trade Commission, Federal Communications Commission, or the Securities and Exchange Commission; however, this exclusion does not apply to a “privacy regulatory proceeding”.
18. Any “claim” based upon, arising from or involving:
- a. Any employer-“employee” relations, policies, practices, acts or omissions;
 - b. Any actual or alleged refusal to employ any person; or
 - c. Any misconduct with respect to any “employee”.

However, this exclusion does not apply to a “privacy and security claim” or “privacy regulatory proceeding” for, based upon or arising from a “privacy breach” of the “personally identifiable information” of an “employee”.

19. Any “claim” based upon, arising from or involving any actual or alleged harassment or discrimination of any kind including, but not limited to, age, color, race, gender, creed, national origin, marital status, sexual preferences, disability or pregnancy.
20. Any “claim” based upon, arising from or involving:
- a. Any violation of any pension, healthcare, welfare, profit sharing, mutual or investment plan, fund or trust; or
 - b. Any violation of any provision of the Employee Retirement Income Security Act of 1974 and its amendments, or the Pension Protection Act of 2006 and its amendments, or any regulation, ruling or order issued pursuant to the foregoing statutes.

However, this exclusion does not apply to a “privacy and security claim” or “privacy regulatory proceeding” that is based upon or arising from a “privacy breach” of the “personally identifiable information” of any “employee”.

21. Any “claim” based upon, arising from or involving:

- a.** Any actual or alleged unfair competition, price fixing, deceptive trade practices or restraint of trade; or
- b.** Any violation of any antitrust statute, legislation or regulation.

However, this exclusion does not apply to:

- a.** Allegations of unfair competition that form a part of a “media claim”; or
- b.** Allegations of deceptive trade practices that form a part of a “privacy and security claim”.

22. Any “claim” based upon, arising from or involving any actual or alleged infringement of any patent.

23. Any “claim” based upon, arising from or involving the misappropriation, theft, copying, display or publication of any trade secret; however, this exclusion does not apply to a “privacy and security claim” alleging failure to prevent the misappropriation of a trade secret which results from a “privacy and security wrongful act”.

24. Any “claim” based upon, arising from or involving any actual or alleged violation of the Telephone Consumer Protection Act (47 U.S.C. §227), the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108), or the CAN-SPAM Act (15 U.S.C. §§ 7701-7713), each as amended, or any regulations promulgated under the foregoing statutes, or any similar federal, state, local or foreign law, whether such law is statutory, regulatory or common law, including any anti-spam law or other law concerning the use of telephonic or electronic communications for solicitation purposes, or any allegations of invasion or violation of any rights to privacy derived therefrom.

25. Any “claim” based upon, arising from or involving any actual or alleged inaccurate, inadequate or incomplete description of the price of goods, “products” or services.

26. Any “claim” based upon, arising from or involving any violation of any economic or trade sanctions by the United States government including, but not limited to, sanctions administered and enforced by the United States Treasury Department’s Office of Foreign Assets Control (OFAC); however, this exclusion does not apply to a “security breach” originating from any country where the United States of America has imposed economic or trade sanctions.

27. Any “claim” for, based upon, arising from or involving loss of income caused by, or resulting from, “unauthorized trading”.

28. Any “claim” for, based upon, arising from or involving:

- a.** Any actual or alleged loss of value of any “securities”;
- b.** Any actual or alleged purchase or sale of “securities”;
- c.** Any offer of, or solicitation of an offer, to purchase or sell “securities”; or
- d.** Any violation of any “securities” law including, but not limited to, the provisions of the Securities Act of 1933, the Securities Exchange Act of 1934 or the Sarbanes-Oxley Act of 2002, or any regulation promulgated under the foregoing statutes, or any federal, state, local or foreign law similar to the foregoing statutes, including any “Blue Sky” law, whether such law is statutory, regulatory or common law.

29. Any “claim” for, based upon, arising from or involving any actual or alleged warranties or representations made at any time with respect to the fitness, quality, durability, performance or use of “products”, or the providing of, or failure to provide, warnings or instructions for “products”.

30. Any “claim” for any “loss”, cost, “damage” or expense:

- a.** Directly or indirectly caused by, resulting from or in connection with any “war”;
- b.** Resulting from a “cyber operation” carried out as part of any “war”; or
- c.** Resulting from a “cyber operation” that causes a sovereign state to become an “impacted state”.

However, this exclusion does not apply to an “act of cyber terrorism”. Paragraph **c.** above shall not apply to the direct or indirect effect of a “cyber operation” on an “insured computer system” that is not physically located in an “impacted state” but is affected by a “cyber operation”.

31. Any “claim” based upon, arising from or involving a “widespread event”. The determination of what 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”.

SECTION III – 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”, “claims” or Coverages.

1. First Party Loss Coverage Limit of Insurance

The First Party Loss Coverage Limit of Insurance shown in the Schedule is the most “we” will pay under the First Party Loss Coverage for all “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 “insureds”, “insured events” or Coverages. All “loss” paid under the First Party Loss Coverage Limit of Insurance will reduce and may completely exhaust the Combined Aggregate Limit shown in the Schedule.

2. Third Party Claims Coverage Limit of Insurance

The Third Party Claims Coverage Limit of Insurance shown in the Schedule is the most “we” will pay under the Third Party Claims Coverage for “legal expenses” and “loss” arising from any one “claim” first made during the “policy period”, and in the aggregate for all “claims” first made during the “policy period”, regardless of the number of “insureds”, “claims” or Coverages. All “legal expenses” and “loss” paid under the Third Party 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:

- a. “Loss” under the First Party Loss Coverage; and
- b. “Legal expenses” and “loss” under the Third Party Claims Coverage.

If the Combined Aggregate Limit is paid, “our” obligations under this Coverage Part will be fully extinguished.

4. Related Claims

- a. “Loss” resulting from a series of similar, related or repeated “insured events” committed by one or more persons, or by a person or persons aiding, abetting or acting in collusion with others against an “insured”, will be 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 an “insured” on the date the first “insured event” in that series was first discovered by an “insured” 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 “claims” arising from the same “wrongful act”, or a series of related “wrongful acts”, will be deemed to be a single “claim”; will be deemed to have been first made against an “insured” on the date the earliest of such “claims” was first made against an “insured”; and will be deemed to have been first reported to “us” on the date the earliest of such “claims” was first reported to “us” in writing. Appeals and any post-trial proceedings or consolidated proceedings approved by us will be part of the original “claim”.
- c. If an “insured event” reported to “us” under the First Party Loss Coverage results in a “claim” under the Third Party Claims Coverage, such matters will be deemed to be related, even if the “claim” is made against an “insured” in a subsequent “policy period”. Such “claim” will be subject to the Limits of Insurance of the “policy period” in effect when the “insured event” giving rise to the “claim” was first discovered by an “insured”.

SECTION IV – CONDITIONS

1. Other Insurance

The coverage provided by this Coverage Part is excess insurance over any other valid and collectible insurance available to an “insured”, 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. Duties in the Event of a Privacy and Security Claim or Insured Event

- a. An “insured” must notify “us” of a “claim” or “insured event” as soon as practicable during the “policy period”, but no later than 60 days after expiration or termination of the “policy period”.
- b. An “insured” must notify law enforcement authorities of any “insured event” as soon as possible.
- c. An “insured” must immediately send us copies of any demands, notices, summonses or legal papers that an “insured” receives in a connection with a “claim”.
- d. In the event of “credit card fraud”, an “insured” must notify the issuing credit card company or bank of the facts and circumstances surrounding such “credit card fraud” as soon as possible.

- e. All “insureds” 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 “claim” or “insured event” or proof of “loss”.
- f. All “insureds” must cooperate with “us” fully and authorize “us” to obtain records and other information.
- g. All “insureds” must assist “us”, upon “our” request, in the enforcement of any right against any person or organization which may be liable to an “insured” because of “loss” or “legal expenses” to which this insurance applies.

3. Loss Determination

a. Digital Assets Loss

“Digital assets loss” will be determined as follows:

- (1) If the impacted “digital asset” was purchased from a “third party”, “we” will pay only the lesser of the original purchase price of the “digital asset” or the reasonable and necessary “digital assets loss”.
- (2) If it is determined that the “digital asset” cannot be replaced, restored or recreated, “we” will only pay the actual and necessary “digital assets loss” incurred up to such determination.

b. Income Loss

“Income loss” will be calculated as:

- (1) “Your” net profit, as could have been reasonably projected, but which has been lost as a direct result of a “system failure”; plus
- (2) Any fixed operating expenses (including ordinary payroll) incurred, but only to the extent that such operating expenses must continue during the “period of restoration”.

In calculating “income loss”, “we” will consider the following:

- (1) The prior experience of “farming operations” before the date of the “system failure”, and “your” likely net profit, had no “system failure” occurred;
- (2) Income derived from substitute methods, facilities or personnel used by “you” to maintain “your” revenue stream; and
- (3) “Your” documentation of the trends in “farming operations” and variations in or other circumstances affecting “farming operations” before or after the “system failure”, which would have affected “farming operations” had no “system failure” occurred.

For purposes of calculating “income loss”, “your” net profit will include the amount paid or payable to “you” for goods or “products” that are sold in the normal course of “farming operations”.

c. Brand Loss

“Brand loss” will be calculated by considering:

- (1) The prior experience of “farming operations” before the date of the “adverse media report” or “notification”, whichever applies, and “your” likely net profit had no “adverse media report” been published or “notification” occurred;
- (2) Income derived from substitute methods, facilities or personnel used by “you” to maintain “your” revenue stream;
- (3) “Your” documentation of the trends in “farming operations” and variations in or other circumstances affecting “farming operations” before or after the “adverse media report” or “notification”, which would have affected “farming operations” had no “adverse media report” been published or “notification” occurred; and
- (4) Any fixed operating expenses (including ordinary payroll), but only to the extent that such operating expenses must continue during the “period of indemnity”.

For purposes of calculating “brand loss”, “your” net profit will include the amount of “money” paid or payable to “you” for goods or “products” that are sold in the normal course of “farming operations”.

4. 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”).

5. 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.

6. 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.

7. 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”.

8. 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 “claim “you” 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. “You” are 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 8.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”, “you” 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.

9. Cancellation and Non-Renewal

This Coverage Part may not be canceled separately from the Policy. However, “you” 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 V – DEFINITIONS

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

1. “Acquiring bank” means a bank or financial institution that accepts credit or debit card payments, including stored value cards and pre-paid cards, for goods or services on behalf of a merchant, including processing and crediting those payments to a merchant’s account.
2. “Act of cyber terrorism” means the premeditated use of disruptive activities, or an explicit threat to use disruptive activities, against a computer, “computer system”, or network by a person or group to further social, political, religious or ideological objectives; provided that such activities are not committed by, or at the express direction of, a sovereign state or a government simultaneously engaged in “war” or a “cyber operation” carried out as part of any “war”.
3. “Adverse media report” means a report or communication of an actual or potential “security breach” or “privacy breach” which has been publicized through any media channel, including, but not limited to, television, “print media”, radio or electronic networks, the internet or electronic mail, and threatens material damage to “your reputation” or “your” brand.

4. "Assumed under contract" means liability for "damages" resulting from a "media wrongful act", "security breach" or "privacy breach", where such liability has been assumed by "you" in the form of a written hold harmless or indemnity agreement, but only if such agreement was executed before the "media wrongful act", "security breach" or "privacy breach" occurred.
5. "Attack vector" means the method or combination of methods that are used in a "hacking attack".
6. "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".
7. "Auto" means a land motor vehicle, trailer or semitrailer designed for travel on public roads, including any attached machinery or equipment; or any other land vehicle that is subject to a compulsory insurance or financial responsibility law or other motor vehicle insurance law in the state where it is licensed or principally garaged. "Auto" does not include "mobile equipment".
8. "Bodily injury" means physical injury, sickness, disease or death sustained by any personal and, where resulting from such physical injury only, mental anguish, mental injury, shock, humiliation or emotional distress.
9. "Bodily injury or property damage claim" means a "suit" alleging "bodily injury" or "property damage" that solely and directly results from a "security breach".
10. "Bodily injury or property damage claims sublimit" means the total amount "we" will pay for "damages" and reasonable and necessary "legal expenses" that an "insured" incurs in a "bodily injury or property damage claim" first made during the "policy period", and in the aggregate for all "bodily injury or property damage claims" first made during the "policy period". The "bodily injury or property damage claims sublimit" is part of, and will reduce, the Farm CyberPlus™ Third Party Claims Coverage Limit of Insurance shown in the Schedule.
11. "Brand loss" means "your" net profit, as could have reasonably been projected immediately prior to "notification", or in the event of an "adverse media report", immediately prior to the publication of an "adverse media report", but which has been lost during the "period of indemnity" as a direct result of such "adverse media report" or "notification". "Brand loss" will be determined in accordance with Section **IV.3.c.** of this Coverage Part, but does not include:
 - a. "Public relations expenses"; or
 - b. Any amounts incurred due to an "adverse media report" that also affects or refers in similar terms to a general security issue, an industry, or "your" specific competitors without any specific allegations regarding a "security breach" or "privacy breach".
12. "Breach support and credit monitoring expenses" means those reasonable and necessary expenses that an "insured" incurs, and those, "you" incur on "your" own behalf, or on behalf of a party for whom "you" are "vicariously liable", to provide support activity to parties affected by a "privacy breach", including the cost to set up a call center and to provide a maximum of 12 months of credit monitoring services or credit or identity repair and restoration services.
13. "Business" means any employment, trade, occupation, profession, operation, enterprise or activity intended to realize a benefit or financial gain, whether engaged in on a full-time, part-time, occasional or temporary basis; however, "business" expressly excludes "farming operations".
14. "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, d/b/a, federal or state tax identification number, or other "business" records or information to establish credit accounts, secure loans or enter into contracts.
15. "Card association" means Visa International, MasterCard, Discover, JCB, American Express and any similar credit or debit card association that is a participating organization of the Payment Card Industry Security Standards Council.
16. "Claim" means solely with respect to the Third Party Claims Coverages, respectively, a "media claim"; a "privacy and security claim"; a "privacy regulatory proceeding"; a "PCI DSS claim" and a "bodily injury or property damage claim". A "claim" will be deemed to be first made or instituted against an "insured" when such "claim" is first received by an "insured".
17. "Cloud provider" means any "third party" that provides computing resources to "you" that are delivered as a service over a network or the internet (commonly known as "cloud computing"), including Software as a Service, Platform as a Service and Infrastructure as a Service.
18. "Computer system" means an interconnected electronic, wireless, web or similar system, including all computer hardware and software, used to process and store "data" or information in an analogue, digital, electronic or wireless format, including, but not limited to, computer programs, "data", operating systems, firmware, servers, media libraries, associated input and output devices, any "connected device", networking equipment, websites, extranets, off-line storage facilities (to the extent that they hold "data"), electronic backup equipment and industrial control systems.

19. "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 "auto", "farm equipment", aircraft or watercraft.
20. "Covered bank account" means a bank account maintained by an "insured" at a financial or banking institution, from which the "insured" may request the transfer, payment or delivery of "money" or "securities". "Covered bank account" does not include any "cryptocurrency" account.
21. "Credit card fraud" means the loss, theft or unauthorized and fraudulent use of an "insured's" credit, debit or bank card by a "third party". "Credit card fraud" does not include the use of an "insured's" credit, debit or bank card by another "insured" without permission.
22. "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).
23. "Cryptocurrency" means a medium of exchange that is digital and decentralized, uses blockchain to manage and record transactions and is stored by a "cryptocurrency exchange". "Cryptocurrency" includes, but is not limited to, Bitcoin and Ethereum. "Cryptocurrency" does not include "money" or "securities".
24. "Cryptocurrency crime event" means an "insured's" loss of "cryptocurrency" which is fraudulently taken from the "insured" as a direct result of a "hacking attack".
25. "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".
26. "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.
27. "Cyber bullying expenses" means any of the following directly resulting from a "cyber bullying incident":
 - a. Reasonable and customary charges for the services of a "therapist", when incurred by a "victim" within 12 months after the "cyber bullying incident" is discovered;
 - b. Lost salary or wages, up to a maximum of \$15,000 per "victim" and subject to the Limit of Insurance, resulting from 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, up to a maximum of \$15,000 and subject to the Limit of Insurance, when incurred by a "victim" within 120 days after the "cyber bullying incident" is discovered;
 - d. Reasonable and necessary expenses to temporarily relocate, up to a maximum of \$15,000 and subject to the Limit of Insurance, when incurred by a "victim" within 120 days after the "cyber bullying incident" is discovered;
 - e. If the "victim" is a "minor", reasonable temporary private tutoring expenses, unreimbursed tuition or increase in tuition, up to a maximum of \$15,000 and subject to the Limit of Insurance, to relocate the "minor" to another school, when incurred within 120 days after the "cyber bullying incident" is discovered; and
 - f. Reasonable and necessary fees and costs incurred by a "victim" to retain a digital forensic analyst or professional cyber security consultant.
28. "Cyber bullying incident" means "cyber bullying" directed against an "insured" which causes such "insured" to suffer mental anguish or mental injury, as diagnosed by a "therapist".
29. "Cyber crime event" means:
 - a. "Wire transfer fraud";
 - b. A "phishing attack" directed at an "insured", which fraudulently induces such "insured" to transfer or pay "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 account" as a result of a "hacking attack".
30. "Cyber extortion expenses" means reasonable and necessary costs and expenses, other than "cyber extortion monies", that an "insured" incurs as a direct result of a "cyber extortion threat", including the cost to hire a "third party" specializing in IT security to determine the validity and severity of a "cyber extortion threat".

31. "Cyber extortion monies" means "money", cryptocurrency or "other property" that an "insured" pays to a person or group reasonably believed to be responsible for a "cyber extortion threat" to prevent or terminate such "cyber extortion threat".
32. "Cyber extortion threat" means a credible threat, or a series of related credible threats, including a demand for "cyber extortion monies", which is directed at an "insured" to:
 - a. Steal, alter, release, divulge, destroy, disseminate, publicly disclose or misuse "private information" taken from an "insured" as a result of unauthorized access to, or unauthorized use of, an "insured computer system";
 - b. Introduce a "virus" into an "insured computer system",
 - c. Corrupt, damage, disable or destroy an "insured computer system",
 - d. Deny, restrict or hinder access to an "insured computer system", including the threat of a "denial of service attack",
 - e. Perpetrate or carry out a "phishing attack";
 - f. Steal, alter, release, reveal, divulge, disseminate, destroy, publicly disclose or misuse the "personally identifiable information" of an "insured"; or
 - g. Damage "your reputation" or "your" brand by posting false or misleading comments about "you" or "farming operations" on social media websites or platforms.
33. "Cyber operation" means the use of a "computer system" by, at the direction, or under the control of a sovereign state to disrupt, deny, degrade, manipulate or destroy information in a "computer system" of or in another sovereign state.
34. "Damages" means a monetary judgment, award or settlement that an "insured" is legally obligated to pay because of a "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; any amounts deemed uninsurable under applicable law; any "insured's" future profits or royalties, restitution, or disgorgement of any profits, remuneration or financial advantage to which an "insured" was not legally entitled; the loss of any "insured's" fees or profits; or the return or offset of any "insured's" fees, charges, commissions or royalties provided or contracted to be provided.
35. "Data" means any machine-readable information, including, but not limited to, ready-for-use programs, applications, account information, customer information, health and medical information or other electronic information, irrespective of the way it is used and rendered.
36. "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 "computer system" by sending an excessive volume of "data" to such "computer system" to deny, restrict or hinder access to such "computer system".
37. "Digital assets" means "data" and computer programs that exist in an "insured computer system". "Digital assets" does not include computer hardware.
38. "Digital assets loss" means reasonable and necessary expenses and costs that an "insured" incurs to replace, recreate or restore "digital assets" to the same state and with the same contents immediately before the "digital assets" were damaged, destroyed, altered, misused or stolen, including expenses for materials and machine time. With respect to "you" only, "digital assets loss" also includes amounts representing "employee" work time to replace, recreate or restore "digital assets", which will be determined on a predefined billable hour or per-hour basis as based upon "your" schedule of "employee" billable hours.

"Digital assets loss" will be determined in accordance with Section IV.3.a. of this Coverage Part, but does not include:

 - a. The cost of restoring, updating or replacing "digital assets" to a level beyond that which existed prior to the "system failure";
 - b. Physical damage to, or the costs to repair or replace, any computer hardware or "data" center;
 - c. The economic or market value of "digital assets";
 - d. Costs or expenses incurred to identify, patch or remediate software "programming errors" or system vulnerabilities;
 - e. Costs to upgrade, redesign, reconfigure or maintain an "insured computer system" to a level of functionality beyond that which existed prior to the "system failure"; or
 - f. The cost of restoring, replacing or repairing any electronic media.
39. "Domestic partner" means any person qualifying as such under the provisions of any applicable federal, state or local law.

40. "Employee" means any individual whose labor or service is engaged by and directed by "you", including volunteers, interns and part-time, seasonal, temporary or leased workers. "Employee" does not include any independent contractor.
41. "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.
42. "Family member" means any of the following persons residing with "you":
- "Your" spouse or registered "domestic partner";
 - Any "minor"; and
 - Other persons related to "you" by blood, marriage or adoption.
43. "Farm equipment" means "mobile equipment" and drones that connect to the internet or to other electronic devices, are owned by, or leased to, "you" and operated under an "insured's" control and are used solely in connection with "farming operations". "Farm equipment" does not include any "auto", aircraft other than drones, or watercraft.
44. "Farm premises" means:
- The premises that are described on the Declarations and used by "you" for "farming";
 - Other land that "you" rent, lease or control and use for "farming";
 - New premises that are acquired by "you" during the "policy period" for "farming"; and
 - Private access ways immediately adjoining the locations described in **a.**, **b.**, and **c.** above.
45. "Farming" means the planting, growing and harvesting of crops or the breeding, raising and care of livestock or poultry. "Farming" does not include the use of any premises, site or location for any "business" activity or any farm-related education, promotion, recreation, entertainment or tourism that is undertaken for money or other compensation.
46. "Farming operations" means "your" farming on the "farm premises". "Farming operations" also includes "your" operation of roadside stands that are maintained solely for the sale of "your" farm "products".
47. "Financial fraud loss" means an "insured's" loss of "money" or "securities" which is fraudulently taken from an "insured" as a direct result of a "cyber crime event".
48. "Forgery" means the alteration of an "insured's" negotiable instrument, or the imitation of an "insured" on a negotiable instrument, with instructions to pay, including counterfeit items, and with the intent to deceive.
49. "Hacking attack" means any of the following directed at or enacted upon an "insured computer system":
- Unauthorized access to, or unauthorized use of, an "insured computer system", including any such unauthorized access or unauthorized use resulting from the theft of a password from an "insured computer system" or from an "insured";
 - A "denial of service attack" on an "insured computer system";
 - Infection of an "insured computer system" by a "virus", or the transmission of a "virus" from an "insured computer system"; or
 - An "act of cyber terrorism".
50. "Identity theft" means the act of knowingly transferring or using, without lawful authority, a means of an "insured's" personal identification, with the intent to commit a crime, or aid or abet another to commit a crime, including the fraudulent use of an "insured's" personal identity to establish credit accounts, secure loans or enter into contracts. "Identity theft" includes the fraudulent use of an "insured's" health insurance numbers to file false health insurance claims or to seek medical treatment or prescription drugs. "Identity theft" does not include "business identity theft".
51. "Identity theft expenses" means any of the following incurred by an "insured" because of "identity theft":
- Reasonable and customary notary and certified mail charges for completing and delivering fraud affidavits to law enforcement agencies, credit agencies, health insurance companies, healthcare providers, merchants, or financial institutions or similar credit grantors;
 - 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. 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 an “insured’s” identity or credit history, or otherwise resolve the “identity theft”, up to a maximum payment of \$200 per day and subject to the Limit of Insurance; however, “our” total payment for lost wages or earnings will not exceed \$5,000 in any one “policy period”;
 - d. Reasonable and customary daycare and eldercare costs, if such care is necessary for an “insured” 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 an “insured’s” identity or credit history, or otherwise resolve the “identity theft”, up to a maximum of \$1,000 per week for up to 5 weeks and subject to the Limit of Insurance; however, such care must be provided by a professional care provider who is not a “family member”;
 - e. Reasonable and customary travel and accommodations expenses incurred by an “insured” in the process of resolving “identity theft”, up to a maximum limit of \$1,000 per week for up to five weeks and subject to the Limit of Insurance;
 - 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, or financial institutions or similar credit grantors to report or discuss “identity theft”;
 - g. “Attorney” fees and associated costs to:
 - (1) Defend lawsuits brought against an “insured” by merchants, financial institutions or their collection agencies;
 - (2) Remove criminal or civil judgments wrongly entered against an “insured” 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 an “insured” as a result of “identity theft”;
 - (6) Contest the wrongful transfer of ownership of an “insured’s” tangible property; or
 - (7) Provide an “insured” 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 credit reports from established credit bureaus; however, such credit reports must be dated no later than 12 months after an “insured” first discovers the “identity theft”, and no more than two credit reports may be obtained from any one established credit bureau; and
 - k. Reasonable and customary credit monitoring costs for up to 24 months; however, such credit monitoring must begin no later than six months after an “insured” first discovers the “identity theft”.
- 52.** “Impacted state” means a sovereign state where a “cyber operation” has had a major detrimental impact on the following:
- 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.
- 53.** “Income loss” means the net profit loss “you” sustain during the “period of restoration” as a direct result of a “system failure”. “Income loss” will be determined in accordance with Section **IV.3.b.** of this Coverage Part, but does not include loss of goodwill or harm to “your reputation”.
- 54.** “Insured” means “you”. “Insured” also includes:
- a. If “you” are an individual, any “family member”; and
 - b. Solely with respect to the Third Party Claims Coverage:
 - (1) Any “employee”, but only with respect to their duties in conducting “farming operations”;

- (2) If “you” are a partnership, joint venture or limited liability company, “your” managers, partners and members, but only with respect to their duties in conducting “farming operations”;
- (3) If “you” are an organization other than a partnership, joint venture or limited liability company:
 - (a) “Your” current officers or directors, but only with respect to their duties in conducting “farming operations”; and
 - (b) “Your” stockholders, but only with respect to their liability as stockholders.

55. “Insured computer system” means:

- a. Any “computer system” operated by, and either owned by or leased to, an “insured”;
- b. With respect to “privacy and security claims” only, “insured computer system” also includes a “computer system” operated by an “outsourced IT service provider”, which is used to provide services to “you” or for processing, maintaining, hosting or storing “data” for “you”, pursuant to a written contract with “you” to provide such services; and
- c. With respect to “bodily injury or property damage claims” only, “insured computer system” also includes “farm equipment”.

56. “Insured event” means solely with respect to the First Party Loss Coverages, respectively, “identity theft”; a “system failure”; “credit card fraud” or “forgery”; a “cyber crime event”; a “cryptocurrency crime event”; a “cyber extortion threat”; a “cyber bullying incident”; an “adverse media report”; or “security breach” or privacy breach”; and “a privacy breach” or “security breach”.

57. “Interruption expenses” means those reasonable and necessary expenses, excluding “special expenses”, incurred by “you” to avoid or minimize the suspension of “farming operations” because of a total or partial interruption, degradation in service, or failure of an “insured computer system” caused by a “system failure”, which “you” would not have incurred in the absence of a “system failure”. “Interruption expenses” include, but are not limited to, the use of rented/leased external equipment, substitution of other work or production procedures, use of “third party” services, or additional staff expenditures or labor costs. The amount of “interruption expenses” recoverable shall not exceed the amount by which the covered “income loss” is reduced by such incurred expenses.

58. “Legal expenses” means reasonable and necessary “attorney” fees for legal services rendered and associated costs and expenses incurred by an “insured” in the defense of a “claim”. “Legal expenses” does not include retainers or any advanced costs.

59. “Loss” means solely with respect to the First Party Loss Coverages, respectively, “identity theft expenses”; “digital assets loss” and “special expenses”; “income loss”, “interruption expenses” and “special expenses”; an “insured’s” loss of “money” as a direct result of “credit card fraud” or “forgery”; “financial fraud loss” an “insured’s” loss of “cryptocurrency” as a direct result of a “cryptocurrency crime event”; “cyber extortion expenses” and “cyber extortion monies”; “cyber bullying expenses”; “privacy breach response costs”, “notification expenses” and “breach support and credit monitoring expenses”; and “brand loss”; and solely with respect to Third Party Claims Coverages, respectively: “damages” and “legal expenses”; “damages” and “legal expenses”, “regulatory compensatory awards” and “regulatory fines and penalties”; and “PCI DSS fines and assessments” and “legal expenses”; and “damages” and “legal expenses”.

60. “Media claim” means a “suit” alleging a “media wrongful act”.

61. “Media material” means communicative material of any kind or nature for which “you” are responsible, including, but not limited to, words, pictures, sounds, images, graphics, code and “data”, regardless of the method or medium of communication of such material or the purpose for which the communication is intended. “Media material” does not include any “products”.

62. “Media wrongful act” means any of the following, whether actual or alleged, but only if directly resulting from the dissemination of “media material” by an “insured” in the conduct of “farming operations”:

- a. Any form of defamation or other tort related to the disparagement or harm to the reputation or character of any person or organization, including libel, slander, product disparagement or trade libel, and infliction of emotional distress, mental anguish, outrage or outrageous conduct, if directly resulting from any of the foregoing;
- b. Invasion, infringement or interference with an individual’s right of privacy or publicity, including the torts of false light, intrusion upon seclusion, commercial misappropriation of name, person or likeness, and public disclosure of private facts;
- c. Plagiarism, piracy or misappropriation of ideas under an implied contract;
- d. Infringement of copyright, trademark, trade name, trade dress, title, slogan, service mark or service name;

- e. Domain name infringement or improper deep-linking or framing;
 - f. Negligence in “media material”, including a “media claim” alleging harm to any person or entity that acted or failed to act in reliance upon such “media material”;
 - g. False arrest, detention or imprisonment;
 - h. Trespass, wrongful entry or eviction, eavesdropping or other invasion of the right of private occupancy; or
 - i. Unfair competition, but only when arising out of a peril described in paragraphs a. through h. above.
- 63.** “Merchant services agreement” means an agreement between “you” and an “acquiring bank”, “card association”, brand, network, credit or debit card processor, independent sales organization, gateway or membership service, which enables “you” to accept payment by credit card, debit card or prepaid card.
- 64.** “Minor” means any person under 21 years of age who is related to “you” by blood, marriage, adoption or legal guardianship.
- 65.** “Mobile equipment” means any of the following types of land vehicles, including any attached machinery or equipment:
- a. Bulldozers, farm machinery, forklifts and other vehicles designed primarily for use off public roads;
 - b. Vehicles maintained for use solely on or next to “farm premises”;
 - c. Vehicles that travel on crawler treads;
 - d. Vehicles, whether self-propelled or not, that are designed to be used primarily to provide mobility to permanently mounted power cranes, shovels, loaders, diggers, drills, or road construction or resurfacing equipment such as graders, scrapers or rollers;
 - e. Vehicles not described in **a.**, **b.**, **c.** or **d.** above which are not self-propelled and are used primarily to provide mobility to the following types of permanently attached equipment:
 - (1) Cherry pickers and similar devices used to raise or lower workers; or
 - (2) Air compressors, pumps and generators, including spraying, welding, building cleaning, geophysical exploration, lighting and well servicing equipment; or
 - f. Vehicles not described in **a.**, **b.**, **c.** or **d.** above which are primarily maintained for purposes other than the transportation of persons or cargo.
- “Mobile equipment” does not include “autos” or self-propelled vehicles with the following types of permanently attached equipment:
- a. Equipment designed primarily for snow removal, street cleaning, or road maintenance other than road construction or resurfacing;
 - b. Cherry pickers and similar devices mounted on automobile or truck chassis and used to raise or lower workers; or
 - c. Air compressors, pumps and generators, including spraying, welding, building cleaning, geophysical exploration, lighting and well servicing equipment.
- 66.** “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”.
- 67.** “Notification” means an “insured’s” written notice to affected individuals in the event of a “security breach” or “privacy breach”, whether such written notice is made by the “insured” voluntarily or to company with “privacy regulations”.
- 68.** “Notification expenses” means reasonable and necessary expenses that an “insured” incurs and those “you” incur on “your” own behalf, or on behalf of a party for whom “you” are “vicariously liable”, to provide “notification” of a “security breach” or “privacy breach”, including printing costs, mailing and postage expenses, and the costs to engage a “third party” to mail “notification” letters and prepare substitute or website notices.
- 69.** “Other property” means any tangible property, other than “money” or “securities”, which has intrinsic value.
- 70.** “Outsourced IT service provider” means a “third party” that provides information technology services to “you” in connection with “farming operations”, under a written contract with “you” to provide such services, including, but not limited to, hosting, security management, co-location and “data” storage. “Outsourced IT service provider” includes any “cloud provider”.

- 71.** “PCI Data Security Standard” (known as PCI DSS) means the Payment Card Industry Security Standards Council Data Security Standard in effect now, or as hereafter amended, which all merchants and processors must follow when storing, processing and transmitting cardholder “data”.
- 72.** “PCI DSS claim” means a written demand for “PCI DSS fines and assessments” received by an “insured” directly or indirectly from or through an “acquiring bank”, “card association” or payment card processor due to “your” non-compliance with the “PCI Data Security Standard”, or a request for information received by an “insured” from an “acquiring bank”, “card association” or payment card processor regarding a suspected “security breach” or “privacy breach”.
- 73.** “PCI DSS fines and assessments” means monetary fines, penalties or assessments, including fraud recoveries, card reissuance costs, operational expenses or compliance case costs, which an “insured” is legally obligated to pay under the terms of a “merchant services agreement”, but only where such monetary fines, penalties or assessments result from a “security breach” or “privacy breach”.
- 74.** “Period of indemnity” means the period beginning on the earlier of the date of “notification” or the first “adverse media report” (whichever applies), and ending on the earlier of:
- a.** The date when “your” gross revenues are restored to the level they had been prior to “notification” or the first “adverse media report” (whichever applies); or
 - b.** 180 consecutive days after the date of “notification” or the first “adverse media report” (whichever applies).
- 75.** “Period of restoration” means the period beginning on the date when the “system failure” began and ending on the earlier of:
- a.** The date when the “insured computer system” is restored or could have been repaired or restored with reasonable speed to the same condition, functionality and level of service that existed prior to the “system failure”, plus a maximum of 30 additional consecutive days after restoration of the “insured computer system” to allow for restoration of “farming operations”; or
 - b.** 120 consecutive days after the date when the “system failure” began.
- 76.** “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, bank 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.
- 77.** “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”.
- 78.** “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.
- 79.** “Print media” means newspapers, newsletters, magazines, books and literary works in any form, brochures or other types of publications, and advertising materials including packaging, photographs, and digital images.
- 80.** “Privacy and security claim” means a “suit” alleging a “privacy and security wrongful act”.
- 81.** “Privacy and security wrongful act” means any of the below, whether actual or alleged, but only if committed by an “insured” in the conduct of “farming operations”:
- a.** The failure to prevent or hinder a “security breach”, which in turn results in:
 - (1)** The alteration, copying, corruption, destruction, deletion or damage to electronic “data” stored on an “insured computer system”;
 - (2)** Theft, loss or unauthorized disclosure of electronic or non-electronic “private information” that is in an “insured’s” care, custody or control;
 - (3)** Theft, loss or unauthorized disclosure of electronic or non-electronic “private information” that is in the care, custody or control of an “outsourced IT service provider” that is holding, processing or transferring such “private information” on “your” behalf; provided, however, that the theft, loss or unauthorized disclosure occurs while “your” written contract with such “outsourced IT service provider” is still in effect; or
 - (4)** Unauthorized access to, or unauthorized use of, a “computer system” other than an “insured computer system”;

- b. The failure to timely disclose a “security breach” affecting “private information”;
- c. The failure to dispose of “private information” within the required time period, in violation of “privacy regulations”;
- d. The failure to prevent the transmission of a “virus” from an “insured computer system” to the “computer system” of a “third party”;
- e. A “privacy breach”;
- f. The failure to prevent a “privacy breach”;
- g. The failure to prevent or hinder participation by an “insured computer system” in a “denial of service attack” directed against an internet site or “computer system” of a “third party”;
- h. The failure to prevent the theft or loss of “personally identifiable information” of any “employee”; or
- i. Infliction of emotional distress or mental anguish, but only if directly resulting from a peril described in paragraphs a. through h. above.

“Privacy and security wrongful act” also includes an “insured’s” failure to prevent “cyber bullying” committed by a “minor” or by a person posing as the “insured”.

82. “Privacy breach” means any of the following:

- a. The unauthorized collection, disclosure, use, access, destruction or modification of “private information”;
- b. The inability to access, or failure to provide, “private information”;
- c. The theft or loss of “private information”, including the theft or loss of “private information” that is stored on an unsecured “data” storage device or “connected device” which is owned and operated by “insured”;
- d. The surrender of “private information” in a “phishing attack”;
- e. With respect to “you” only, the failure to implement, maintain or comply with privacy policies and procedures stating “your” obligations regarding “private information”, including but not limited to “your privacy policy”;
- f. The failure to implement specific security practices with respect to “private information”, as required by “privacy regulations”;
- g. An infringement or violation of any rights to privacy;
- h. Breach of a person’s right of publicity, false light, or intrusion upon a person’s seclusion;
- i. The failure to comply with “privacy regulations” pertaining to an “insured’s” responsibilities with respect to “private information”, but only in connection with an act listed in paragraphs a. through h. above; or
- j. With respect to “you” only, the failure to comply with “privacy regulations” prohibiting unfair or deceptive trade practices or consumer fraud pertaining to “your” responsibilities with respect to “private information”, but only in connection with an act listed in paragraphs a. through i. above.

83. “Privacy breach response costs” means:

- a. Reasonable and necessary “public relations expenses” that “you” incur prior to or following the publication of an “adverse media report” to avert or mitigate any material damage to “your reputation” or “your” brand, which results or reasonably could result from an “adverse media report”; and
- b. Reasonable and necessary legal fees that “you” incur to:
 - (1) Determine the scope, cause and extent of an actual or suspected “privacy breach” or “security breach”;
 - (2) Determine the applicability of, and “your” obligations to comply with, “privacy regulations” due to an actual or suspected “privacy breach”; and
 - (3) Draft a “notification” letter to be sent to parties affected by a “privacy breach”;
- c. Reasonable and necessary fees and costs that “you” incur on “your” own behalf, or on behalf of a party for whom “you” are “vicariously liable”, to retain a qualified IT forensics firm or computer security expert to investigate and identify the source and scope of a “security breach” or “privacy breach”; and
- d. Overtime salaries of non-exempt “employees” assigned to handle inquiries from parties affected by a “privacy breach”.

- 84.** “Privacy regulations” means foreign, federal, state or local statutes, rules, regulations and other laws, as they currently exist and as amended, associated with the confidentiality, access, control, and use of “private information”, including, but not limited to:
- a.** The Health Insurance Portability and Accountability Act of 1996 (Public Law 104- 191), known as HIPAA, and related or similar state medical privacy laws;
 - b.** The Gramm-Leach-Bliley Act of 1999 (G-L-B), also known as the Financial Services Modernization Act of 1999, including sections concerning security protection and standards for customer records maintained by financial services companies, and the rules and regulations promulgated thereunder;
 - c.** State and federal statutes and regulations regarding the security and privacy of consumer information;
 - d.** Governmental privacy protection regulations or laws associated with the control and use of “personally identifiable information”, including but not limited to, requirements to post a privacy policy, adopt specific privacy controls, or inform customers of an actual or suspected “privacy breach”;
 - e.** The privacy provisions of consumer protection laws, including the Federal Fair Credit Reporting Act (FCRA) and similar state laws;
 - f.** The Children’s Online Privacy Protection Act or similar laws, as they exist now or in the future;
 - g.** The EU General Data Protection Act or other similar privacy and security statutes, rules, regulations or other laws worldwide, as they exist now or in the future; and
 - h.** The Health Information Technology for Economic and Clinical Health Act (HITECH ACT), enacted under Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5), and its implementing regulations, including related or similar state medical privacy laws.
- 85.** “Privacy regulatory proceeding” means a civil administrative proceeding, regulatory action, request for information or investigation instituted against an “insured” by a foreign, federal, state or local governmental body because of a “security breach” or “privacy breach”.
- 86.** “Private information” means:
- a.** Proprietary or confidential information owned by a “third party” that is in the care, custody or control of an “insured” or is used by an “insured” with the consent of such “third party”;
 - b.** “Personally identifiable information”; and
 - c.** Any other information that is linked or linkable to a specific individual that is subject to any “privacy regulations”.
- 87.** “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.
- 88.** “Products” means any tangible goods or devices that are manufactured, produced, processed, prepared, assembled, packaged, labeled, sold, handled or distributed by “you”; and containers, materials, parts or equipment furnished in connection with such goods or devices.
- 89.** “Programming errors” means errors that occur during the development or encoding of a computer program, software or application and which would, when in operation, result in a malfunction or incorrect operation of a “computer system”.
- 90.** “Property damage” means physical injury to, or impairment, destruction or corruption of, any tangible property, including the loss of use thereof. “Data” is not considered tangible property.
- 91.** “Public relations expenses” means expenses incurred by “you”, including those to hire a “third party” public relations consultant or public relations firm, to protect or restore “your reputation”, which is damaged or reasonably could be damaged as a direct result of an “adverse media report”.
- 92.** “Regulatory compensatory award” means a sum of “money” that an “insured” is legally obligated to pay as a regulatory agency’s award or fund for parties affected by a “privacy breach” due to an adverse judgment or settlement arising out of a “privacy regulatory proceeding”. “Regulatory compensatory award” includes consumer redress funds but does not include any criminal penalties or fines of any nature whatsoever.
- 93.** “Regulatory fines and penalties” means civil fines or penalties imposed by a foreign, federal, state or local governmental regulatory body against an “insured” in a “privacy regulatory proceeding”. “Regulatory fines and penalties” does not include any amounts deemed uninsurable under applicable law or any criminal fines or penalties of any nature whatsoever.

- 94.** “Related hacking attack” means a “hacking attack” with:
- The same actor or coordinated group of actors;
 - The same “attack vector”;
 - The same vulnerability; or
 - 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 “claim” or “insured event”.
- 95.** “Securities” means negotiable or non-negotiable instruments or contracts representing “money” or “other property” but does not include “money” or “cryptocurrency”.
- 96.** “Security breach” means any of the following, whether a specifically targeted attack or a generally distributed attack:
- A “hacking attack”; or
 - The physical theft or loss of an unsecured “data” storage or “connected device” that contains “private information” and is owned and operated by an “insured”.
- 97.** “Special expenses” means reasonable and necessary costs and expenses that an “insured” incurs to:
- Prevent, preserve, minimize or mitigate any further damage to “digital assets”, including the reasonable and necessary fees and expenses of specialists, outside consultants or forensic experts;
 - Preserve critical evidence of any criminal or malicious wrongdoing;
 - Purchase replacement licenses for computer programs because the copy protection system or access control software was damaged or destroyed by a “system failure”; or
 - Notify affected individuals of a total or partial interruption, degradation in service, or failure of an “insured computer system” resulting from a “system failure”.
- 98.** “Suit” means:
- The service of a civil lawsuit or the institution of arbitration or other alternative dispute resolution proceedings against an “insured” seeking “damages” or non-monetary relief; or
 - A written demand made against an “insured” for “damages” or non-monetary relief.
- 99.** “System failure” means an unplanned outage, interruption, failure, suspension, or degradation of service of an “insured computer system”, including, but not limited to, any such outage, interruption, failure, suspension or degradation of service caused directly by a “hacking attack”.
- 100.** “Therapist” means a psychologist or other mental health professional who is licensed or certified under the laws of the jurisdiction in which mental health treatment is given to a “victim” and who is qualified to provide such treatment. “Therapist” does not include any “insured”.
- 101.** “Third party” means any entity, company, organization or person who does not qualify as an “insured” under this Coverage Part.
- 102.** “Unauthorized trading” means trading, which at the time of the trade, exceeds permitted financial limits or is outside of permitted product lines.
- 103.** “Vicariously liable” means “your” legal responsibility for the liability of others, including legal responsibility “you” assume in a contract. The existence of vicarious liability will not create or confer any rights or duties under this Coverage Part to any “third party”, other than as provided in this definition.
- 104.** “Victim” means any “insured” who suffers mental anguish or mental injury as a direct result of a “cyber bullying incident”.
- 105.** “Virus” means malicious software intentionally designed to insert itself by a variety of forms into a “computer system” to damage, destroy, corrupt, overload or otherwise impair the functionality of such “computer system”. “Virus” includes, but is not limited to, worms, Trojan horses, spyware, dishonest adware and malware.

106. “Waiting period” means:

- a.** Solely with respect to First Party Loss, **2.b.** the eight-hour period which must elapse before “income loss”, “interruption expenses” and/or “special expenses” may be payable.
- b.** Solely with respect to First Party Loss **9.**, the two-week period which must elapse after “notification”, or in the event of an “adverse media report”, after publication of the first “adverse media report”, before “brand loss” may be payable.

The “waiting period” applies to each “period of indemnity” or “period of restoration”, whichever applies.

107. “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.

108. “We”, “us” and “our” mean the Company providing the insurance under this Coverage Part.

109. “Widespread event” means 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 then first such person or entity should have discovered, such “hacking attack”.

110. “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” from a “covered bank account”, which instruction purports to have been transmitted by an “insured” but was in fact fraudulently transmitted by a “third party” without an “insured’s” knowledge or consent.

111. “Wrongful act” means solely with respect to Third Party Claims Coverage, respectively: a “media wrongful act”; a “privacy and security wrongful act”; a “security breach” or “privacy breach”; a “security breach” or “privacy breach”; and a “security breach”.

112. “You” and “your” mean any natural person or organization listed as such in the Declarations of the Policy.

113. “Your privacy policy” means “your” published policies which are provided to “employees” or “third parties” in written or electronic form and govern the collection, dissemination, confidentiality, integrity, accuracy or availability of “private information”.

114. “Your reputation” means the estimation of trust that customers or clients have in “farming operations”.

SECTION VI – SERVICE PROVIDERS

- 1.** When an “insured event” is reported to “us”, “we” may suggest service providers. If an “insured” prefers to use an alternative service provider, “our” payment for services provided by any alternative service provider will not exceed the amount that “we” would have paid for the same services using a service provider “we” suggested.
- 2.** The “insured” will have a direct relationship with any service provider used, whether paid for in whole or in part under this Coverage Part. All service providers work for the “insured”.

SECTION VII – ENTIRE AGREEMENT

By acceptance of this Coverage Part, “you” agree that this Coverage Part embodies all agreements between “you” 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”.