CyFlare Security Participant Terms and Conditions

Certification Warranty Program

This Certification Warranty Program (**Certification Warranty)** and the terms and conditions herein (the **Agreement**), is a legal agreement entered into by and between **CYFLARE SECURITY** and the Participant enrolling in the **CYFLARE SECURITY Certification Warranty** (also, **Warranty**) pursuant to the terms herein. This Agreement governs Participant's access to benefits available only through this Certification Warranty. This Agreement is effective on the date **CYFLARE SECURITY** confirms Participant's enrollment in the Certification Warranty and agreement to the terms set forth herein, along with Provider Terms, if any, included on the enrollment portal (**Effective Date**). The enrollment portal is referred to herein as the "Token Portal".

BY ENROLLING IN THE CERTIFICATION WARRANTY PROGRAM AND CLICKING A "SUBMIT", "CONTINUE" OR OTHER SIMILAR BUTTON ASSOCIATED WITH THIS AGREEMENT, PARTICIPANT OR ITS AUTHORIZED AGENT EXPRESSLY AND EXPLICITLY ACKNOWLEDGES AND AGREES (I) IT IS A BUSINESS ENTITY DULY ORGANIZED, VALIDLY EXISTING AND IN GOOD STANDING UNDER THE LAWS OF THE STATE OR COUNTRY IN WHICH IT IS INCORPORATED; (II) THIS IS A BINDING AGREEMENT; (III) PARTICIPANT HAS FULLY IMPLEMENTED SOLUTIONS FROM **CYFLARE SECURITY** FOR ITS ENVIRONMENT; AND (IV) ACCEPTS THE OFFER TO ENROLL IN THE CERTIFICATION WARRANTY PROGRAM PURSUANT TO PROVIDER TERMS AS WELL AS TO THE TERMS HEREIN. PARTICIPANT'S ENROLLMENT IS CONSIDERED ACCEPTED WHEN PARTICIPANT RECEIVES A CONFIRMATION EMAIL FROM CYFLARE SECURITY EVIDENCING PARTICIPANT'S SUCCESSFUL ENROLLMENT. AS A REPRESENTATIVE ENTERING INTO THIS AGREEMENT ON BEHALF OF A PARTICIPANT, YOU HEREBY REPRESENT AND WARRANT TO **CYFLARE SECURITY** AND PROVIDER YOU ARE (A) AUTHORIZED TO ENTER INTO THIS AGREEMENT ON BEHALF OF PARTICIPANT; AND (B) YOU ARE OVER 18 YEARS OLD. IF PARTICIPANT DOES NOT ACCEPT ALL TERMS AND CONDITIONS IN THIS AGREEMENT OR IS NOT AUTHORIZED TO ENTER INTO THIS AGREEMENT, DO NOT ACCEPT THE TERMS OF THIS AGREEMENT.

PARTICIPANT MUST IMMEDIATELY REPORT AN EVENT TO PROVIDER. FAILURE TO REPORT AN EVENT WITHIN FORTY-EIGHT (48) HOURS OF DISCOVERY WILL EXCLUDE THE EVENT FROM CONSIDERATION FOR A RECOVERY BENEFIT. WITHIN FIFTEEN (15) DAYS OF DISCOVERY OF AN ACTUAL OR REASONABLY SUSPECTED EVENT, PARTICIPANT MUST SUPPLY PROVIDER WITH THE REQUESTED INFORMATION TO VALIDATE ANY ALLEGED LOSS OF BUSINESS INCOME AND EVALUATE ANY ASSERTED EVENT OR THE REQUEST FOR RECOVERY BENEFITS WILL BE CLOSED. IF PARTICIPANT FAILS TO DELIVER REQUESTED INFORMATION TO PROVIDER AS SET FORTH HEREIN OR FAILS TO RESPOND FOR MORE THAN THIRTY (30) DAYS AFTER INITIAL PROVISION OF INFORMATION TO PROVIDER, PARTICIPANT'S PROFFERED EVENT WILL BE TREATED AS AN INVALID EVENT INELIGIBLE FOR A RECOVERY BENEFIT PURSUANT TO THIS AGREEMENT. ANY DETERMINATION REGARDING A QUALIFYING EVENT OR THE GRANT OF A RECOVERY BENEFIT, IS MADE AT PROVIDER'S SOLE DISCRETION.

In consideration of the mutual covenants and agreements contained herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. **Definitions.** Any capitalized terms not otherwise defined herein shall have the meaning set forth in the Solutions Agreement with CYFLARE SECURITY, or any similarly intended agreement which governs the delivery of the managed detection and response, managed risk, and/or managed security awareness solutions **(Solutions Agreement)** made by and between Participant and CYFLARE SECURITY, or its authorized managed service provider partner, as applicable, for the delivery of the Solutions.

   a. **BEC Event** means a business email compromise **(BEC)** where a full, unauthorized threat-actor takeover of a Participant account occurs within Participant's Environment. This Warranty does not apply to BEC Events where social engineering results in funds transfer or fraud. To be a Qualifying Event, a BEC Event must result from the compromise of credential or other unauthorized access in and of a Participant's own Environment.

   b. **Benefit End Date** means the last day of Participant's qualifying Subscription Term pursuant to the Solutions Agreement with CYFLARE SECURITY, or any qualifying renewals thereof.

   c. **Benefit Start Date** means the first day of the Enrollment Term as set forth on the Enrollment Confirmation from CYFLARE SECURITY.

d. **Business Income Event** means a Security Breach of Participant's Environment materially effecting business operations resulting in actual, documentable loss of business income (net profit or loss before taxes) that would have been earned had no Security Breach occurred.

e. **Compliance Event** means a BEC Event or Ransomware Event directly resulting in a personal data breach, triggering HIPAA, GDPR, UK GDPR, PCI, OSHA, SEC, FTC, and/or any international, federal, state or other legally required notice and/or reporting requirements, where the sole Recovery Benefit is for immediate legal assessment and emergency response of the Compliance Event. Continuing legal services beyond initial breach assessment, including dealing with the nature of the data breach and any extent of the same, are beyond scope of any Recovery Benefit for this Event.

f. **Cyber Legal Liability Event** means litigation arising directly out of a breach of data privacy and/or data security as a result of a BEC Event or Ransomware Event, arising out of binding statements made regarding data privacy or security on Participant's website where legal defense expenses and settlement costs are incurred.

g. **Enrollment Confirmation** means the email issued by CYFLARE SECURITY to Participant confirming Participant's enrollment in the Certification Warranty upon Participant's enrollment in the Token Portal and sets forth the Benefit Start Date and Certification Warranty Indemnification Level. The Enrollment Confirmation is incorporated into and becomes part of this Agreement.

h. **Enrollment Term** means the period within which Participant may receive Recovery Benefits and which begins on the Benefit Start Date as defined in Section 1(c) and ends upon termination in accordance with Section 11 below. Dependent on the Benefit Start Date, generally the Enrollment Term is equivalent to the annual Subscription Term for pursuant to the Solutions Agreement with CYFLARE SECURITY, or in the case of a multi-year qualifying Subscription, the annual periods within such multi-year Subscription Term.

i. **Environment** means computer systems or networks identified by Participant and for which CYFLARE SECURITY has implemented Solutions. The Warranty applies solely to Environments such Solutions are purchased to secure.

j. **Event** means a Ransomware Event or BEC Event occurring in a Participant's Environment, which may then result in a Business Income Event, Compliance Event or Cyber Legal Liability Event.

k. **Provider** means CYFLARE SECURITY's third party service provider who has contracted with CYFLARE SECURITY to provide Participant with the benefits set forth herein.

l. **Qualifying Event** means a Business Income Event, Compliance Event, Cyber Legal Liability Event resulting from a Ransomware Event or BEC Event occurring in Participant's Environment, which qualifies for a Recovery Benefit. For avoidance of doubt, a Ransomware Event and BEC Event cannot be combined in the same request for a Recovery Benefit.

m. **Ransomware Event** means the unauthorized access to at least one Participant endpoint in the form of ransomware which has caused material harm to Participant, whereby "material harm" must include at least one of the following: (i) the unauthorized acquisition of unencrypted digital data from Participant's Environment that compromises the security, confidentiality, or integrity of personal data or confidential information from Participant's Environment; (ii) public disclosure of personal data or confidential information maintained by Participant; or (iii) the compromise of at least one endpoint in Participant's Environment resulting the blocking of access to such endpoint.

n. **Recovery Benefit** is the funding conferred to the Participant by the Provider upon a Qualifying Event. A Recovery Benefit is limited to supporting repair, remediation, and/or replacement of those parts of Participant's Environment damaged by the Qualifying Event, including, but not limited to, removing and remediating elements that caused such Event. Recovery Benefits apply to immediate recovery services such as initial investigation to determine required services and restoration of Participant's current business systems covered by the Solutions. Continuing investigation concerning the extent of an actual or suspected Event, ongoing negotiations with a threat actor, procurement of new solutions or recovery beyond Participant's Environment, legal evaluation of reporting obligations, or other ongoing breach services, are not eligible for a Recovery Benefit.

o. **Security Breach** means the loss of business income (net profit or loss before income taxes) which would have been earned had no loss occurred as a result of (i) an unauthorized access or use of Participant's Environment resulting from theft of a password from an agent of the Participant; (ii) a denial of service attack affecting Participant's Environment; or (iii) an infection of a part of Participant's Environment by malicious code or the unauthorized transmission of malicious code from the Participant's Environment.

p. **Solutions** means the services for which Participant has engaged CYFLARE SECURITY pursuant to a Solutions Agreement to provide protection for Participant's Environment, as governed pursuant to the Solutions Agreement or similarly intended agreement for delivery of managed detection and response, managed risk, and/or managed security awareness solutions.

2. Certification Warranty

a. Benefit Start Date. Participant's Enrollment Term will begin on the Benefit Start Date.
b. Benefit End Date. Unless otherwise terminated earlier pursuant to Section 10 below, Participant's Enrollment Term will automatically terminate on the Benefit End Date.

3. Certification Warranty Benefits.

a. During the Enrollment Term, Participant may submit a request for a Recovery Benefit by notifying Provider at CLAIMS@CYSURANCE.COM that one of the following Events may have occurred during the Enrollment Term:
   i. Ransomware Event;
   ii. BEC Event;
   iii. Compliance Event;
   iv. Cyber Legal Liability Event; and/or
   v. Business Income Event.

b. Should an Event after review be determined a Qualifying Event, and provided an exclusion set forth in Section 4 below does not apply, Provider will allocate a Recovery Benefit to Participant, subject to the following:

   i. Participant may only seek indemnification for one (1) Qualifying Event during the Enrollment Term;
   ii. Participant must have a commercially reasonable belief that damages resulting from the Event will exceed $5,000 USD or equivalent in applicable foreign currency;
   iii. The Recovery Benefit will not exceed Participant's maximum Certification Warranty Indemnification Level as specified within Participant's Enrollment Confirmation;
   iv. Payment of any applicable deductible;
   v. Application of a Recovery Benefit in the form of cyber-insurance deductible-buy back, subject to the terms and conditions of Participant's cyber-insurance carrier, any terms and conditions of Provider, and review and approval by both Provider and Participant's identified cyber-insurance carrier; and
   vi. The Recovery Benefit is provided in accordance with any additional terms and conditions applicable as specified in the Warranty Confirmation Summary attached hereto as Schedule 1.

4. Recovery Benefit Exclusions. A Recovery Benefit will not be provided if any one or more of the following conditions occur specific to the nature of the loss:

a. Participant fails to take commercially reasonable measures to (i) undertake preventative maintenance, including patching that is up to date within sixty (60) days of the software manufacturer's release cycle; and (ii) implement cloud or other back up measures of Participant's data to allow for recovery from a Ransomware Event;
b. Participant fails to verify wire transfers and routing number changes with the requestor including documented with name and date;
c. Participant fails to deploy multifactor authentication **(MFA)** on email, servers housing proprietary and privacy data, and operating systems essential business operations;
d. Participant fails to deploy industry standard and up-to-date anti-virus or comparable prevention tools on its endpoints;
e. Participant does not have the Solutions actively deployed in the Participant's Environment where the Event occurred, such that CYFLARE SECURITY is receiving supported security relevant telemetry from such environment (i.e., infrastructure or endpoint);
f. Participant is in breach of this Agreement and/or the Solutions Agreement, or this Agreement or Solutions Agreement has terminated or expired;
g. Participant is unable to provide sufficient proof of the Event or cannot verify the Event through log or Event data;

h. If there is a systemic failure of the CyFlare's infrastructure that results in an Event where there is a systemic attack inflicting global widespread harm from commonly used tools and/or a zero-day exploit caused by a flaw in software, hardware or firmware occurring in the Participant's Environment;
i. After notification or an alert of a possible Event to Participant from CYFLARE SECURITY, Participant fails to take reasonable measures or actions to investigate and adequately address the issues prompting the alert in an effort to circumvent or prevent an Event from occurring in Participant's Environment;
j. If a Participant is regulated by HIPAA, PCI, SEC, FTC, GDPR and/or any other international, federal, state or other law, regulation or rule:

    i. Participant has not completed an annual security and data risk assessment or other necessary risk assessments, and documented risks associated therewith;
    ii. Protected health information (**PHI**) or other protected information data inventory has not been fully completed and accounted for prior to an incident and request for a Recovery Benefit;
    iii. Subject to Participant's standard historical employment practices related to HIPAA, GLBA, CCPA, GDPR, UK GDPR or other data protection required training for employees, all of Participant's employees have not completed such necessary training within twelve (12) months prior to any Event;
    iv. Participant has not adopted and adhered to all privacy and security policies, public facing, internal or otherwise, related to any international, federal, state or other legal or related regulatory requirements to which Participant is subject prior to any Event; or
    v. Participant is named as a defendant, respondent, co-defendant or other defending party in a class-action lawsuit resulting from violation of any international, federal, state or other law, regulation or rule arising from or relating to an Event.

k. The Event did not occur during the Enrollment Term;
l. Participant fails to verify Wire Transfers and Routing Number Changes with the requestor including documenting such verification(s) with name and date;
m. Participant does not timely submit the request for a Recovery Benefit for the Event during the Enrollment Term; or
n. Participant has not, with regard to all applicable privacy, data protection or security laws, regulations and rules governing the processing of personal information, (i) conducted an assessment or analysis regarding, (ii) taken steps to assess its risks under, and also (iii) adopted and adhered to privacy, data protection or security laws, prior to any Event.

5. Recovery Benefit Request Requirements.

a. PARTICIPANT MUST IMMEDIATELY REPORT AN EVENT TO PROVIDER. FAILURE TO REPORT AN EVENT WITHIN FORTY-EIGHT (48) HOURS OF DISCOVERY WILL EXCLUDE THE EVENT FROM CONSIDERATION FOR A RECOVERY BENEFIT. WITHIN FIFTEEN (15) DAYS OF DISCOVERY OF AN ACTUAL OR REASONABLY SUSPECTED EVENT, PARTICIPANT MUST SUPPLY PROVIDER WITH THE REQUESTED INFORMATION TO VALIDATE ANY ALLEGED LOSS OF BUSINESS INCOME AND EVALUATE ANY ASSERTED EVENT OR THE REQUEST FOR RECOVERY BENEFITS WILL BE CLOSED. IF PARTICIPANT FAILS TO DELIVER ANY REQUESTED INFORMATION TO PROVIDER AS SET FORTH HEREIN OR FAILS TO RESPOND FOR MORE THAN THIRTY (30) DAYS AFTER INITIAL PROVISION OF INFORMATION TO PROVIDER, PARTICIPANT'S PROFFERED EVENT WILL BE TREATED AS AN INVALID EVENT INELIGIBLE FOR A RECOVERY BENEFIT PURSUANT TO THIS AGREEMENT. ANY DETERMINATION REGARDING A QUALIFYING EVENT OR THE GRANT OF A RECOVERY BENEFIT, IS MADE AT PROVIDER'S SOLE DISCRETION.
b. Participant understands this Agreement is separate and apart from, not affiliated with, and not issued by or part of any insurance product it has purchased, engaged or otherwise obtained. Participant understands it is responsible for reporting Events to its insurance carrier regardless of whether Participant elects to make a request for a Recovery Benefit with Provider for an Event under this Warranty.
c. By submitting a request for a Recovery Benefit and information to Provider, Participant understands and acknowledges that Provider has separate terms and conditions related to privacy and data protection as set forth in Provider's website terms, privacy policies, or other agreements made by and between Participant and Provider which will govern the use and protection of the information. Participant understands and agrees it should review any terms prior to submission of information. In the event Participant requests that CYFLARE SECURITY provide information directly to Provider on Participant's behalf, Participant authorizes and consents to CYFLARE SECURITY sharing the information with Provider, subject to the terms set forth in Section 5(b) and 5(c) of this Agreement.

d. Qualification of a Recovery Benefit made under the Certification Warranty is subject to Provider's standards of review. If Provider denies indemnification to Participant, notwithstanding anything to the contrary in this Agreement, CYFLARE SECURITY shall have no liability to Participant.
e. To qualify for a Recovery Benefit under the Certification Warranty, Participant agrees to:

    i. Provide documentation evidencing the Participant's date of enrollment in the Certification Warranty;
    ii. Preserve and provide log files and information about the symptoms and causes of a network compromise and all other information, documents or things requested by Provider pertaining to the request for Recovery Benefit, and all other information, documents or things requested by Provider to assess the Event; and
    iii. Verify cyber event via log files and/or other documentation of malicious code that resulted in loss of data and/or records that triggered a violation of state and/or federal regulatory enforcement to which Participant is subject;
    iv. Submit all requests for a Recovery Benefit in good faith and shall only submit information that is true and accurate.

6. Additional Services. Following Participant's enrollment in the Certification Warranty, and included with such Warranty, Provider will perform regular scans of Participant's Environment. Results will be provided to CYFLARE SECURITY to augment the external monitoring and risk rating analyses CYFLARE SECURITY delivers to Participant as part of the Solutions. Such results may identify vulnerabilities related to:

a. Network Security
b. DNS Health
c. Patching Cadence
d. IP Reputation
e. Application Security
f. Threat Intelligence
g. Social Intel & Industry Intel
h. Information Leak including Dark Web scanning for credentials
i. Cloud Score

An initial scan will be conducted upon Participant's enrollment in the Certification Warranty and monthly thereafter during the Participant's Enrollment Term. By enrolling in the Certification Warranty, Participant consents to the receipt of such additional services by Provider.

7. Warranty Disclaimer. EXCEPT AS SPECIFICALLY SET FORTH HEREIN, CYFLARE SECURITY MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY TO PARTICIPANT, REGARDING OR RELATING TO THE CERTIFICATION WARRANTY OR ITS SOLUTIONS PROVIDED TO PARTICIPANT UNDER THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE CERTIFICATION WARRANTY WILL MEET PARTICIPANT'S REQUIREMENTS OR THAT THE OPERATION THEREOF OR ACCESS THERETO WILL BE ERROR FREE, CURRENT OR UNINTERRUPTED. FOR THE AVOIDANCE OF DOUBT, THIS CERTIFICATION WARRANTY DOES NOT EXPAND OR INFER ANY WARRANTIES RELATED TO THE SOLUTIONS. TO THE GREATEST EXTENT ALLOWED BY LAW, CYFLARE SECURITY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND WARRANTIES ARISING FROM COURSE OF DEALING, USAGE OR TRADE PRACTICE, EXCEPT TO THE EXTENT THAT ANY WARRANTIES IMPLIED BY LAW CANNOT BE VALIDLY WAIVED.

8. Limitation of Liability. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, FOR ANY CAUSE RELATED TO OR ARISING OUT OF THIS AGREEMENT, WHETHER IN AN ACTION BASED ON A CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR ANY OTHER LEGAL THEORY, HOWEVER ARISING, CYFLARE SECURITYWILL IN NO EVENT BE LIABLE TO CUSTOMER OR ANY THIRD PARTY FOR LOST REVENUES, PROFITS, BUSINESS OR GOODWILL, BREACHES BY PROVIDER, OR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES. IN NO EVENT WILL CYFLARE SECURITY'S LIABILITY EXCEED $100. THESE LIMITATIONS SHALL APPLY WHETHER OR NOT PARTICIPANT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

9. Updates. CYFLARE SECURITY reserves the right to modify this Agreement and any terms related to the Warranty in CYFLARE SECURITY's sole discretion. Should CYFLARE SECURITY make any modifications to the Agreement or the Warranty, CYFLARE SECURITY will post the amended terms at https://enroll.cysurance.com/wp-content/uploads/efs/TANDC/CYFLARE.pdf and will update the Last Updated Date

within such document or provide notification by such other reasonable notification method implemented by CYFLARE SECURITY.

10. Termination.

10.1 Should Participant's Subscription change during the Subscription Term which impacts the Certification Warranty Indemnification Level for which Participant qualifies, the existing Enrollment Term will terminate, and, if applicable, a new token ID will be issued to Participant for the applicable Warranty Indemnification Level. Participant must re-enroll on the Token Portal to qualify for the new Warranty Indemnification Level. In the event Participant's Subscription ceases to qualifies for the Warranty, the Enrollment Term will immediately terminate.

10.2 This Agreement, the Certification Warranty, and/or Participant's Enrollment Term may be terminated by CYFLARE SECURITY for convenience and for any reason in CYFLARE SECURITY's sole discretion and CYFLARE SECURITY will have no further liabilities to Participant under this Agreement. CYFLARE SECURITY will use commercially reasonable efforts to notify Participant of any such termination. For the avoidance of doubt, termination of the Solutions Agreement shall terminate this Agreement, but termination of this Agreement shall not terminate the Solutions Agreement.

11. Survival. The definitions in Section 1, along with Sections 4, 5, 7, 8, 9, 11 and 12 will survive the non-renewal or termination of this Agreement.

12. Miscellaneous.

12.1 Except as otherwise provided herein, all notices, consents, demands, waivers and other communications other than a submission of an Event hereunder, shall be in writing and shall be deemed to have been given: (i) when delivered by hand (with written confirmation of receipt); (ii) on the next business day after the date sent, if sent for overnight delivery by a generally recognized international courier (e.g., FedEx, UPS, DHL, etc.) (receipt requested); or (iii) on the date sent by e-mail (with confirmation of transmission) if sent during normal business hours of the recipient, and on the next business day if sent after normal business hours of the recipient. CYFLARE SECURITY's address for notification purposes shall be: CYFLARE SECURITY. Provider's address for notification purposes shall be legal@cysurance.com. Participant's address for notification purposes shall be as provided by Participant to Provider, as well as CYFLARE SECURITY at the time of subscription to the Solutions. Either party may update its notice address upon written notice to the other party.

12.2 Provider is not responsible for failures or delays resulting from events outside of Provider's control.

12.3 No failure or delay by CYFLARE SECURITY or Provider in exercising any right, power or privilege hereunder shall operate as a waiver thereof nor shall any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any other right, power, or privilege.

12.4 Participant shall not be entitled to assign, subcontract, delegate or otherwise transfer any of its rights and/or duties arising out of this Agreement and/or parts thereof to third parties, voluntarily or involuntarily, including by change of control, operation of law or any other manner, without CYFLARE SECURITY's express prior written consent. Any purported assignment, subcontract, delegation, or other transfer in violation of the foregoing shall be null and void.

12.5 Unless otherwise prohibited by law, (i) this Agreement shall be governed by the laws of the State of Delaware without regard to the conflicts of law provisions thereof and (ii) any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be settled by arbitration in Kent County, Delaware in English and in accordance with the JAMS International Arbitration Rules then in effect. Any judgment on the award rendered by the arbitrator may be entered in any court having jurisdiction thereof. Notwithstanding the foregoing, each party shall have the right to institute an action in a court of proper jurisdiction for preliminary injunctive relief pending a final decision by the arbitrator(s), provided that a permanent injunction and damages shall only be awarded by the arbitrator(s). In any action or proceeding to enforce rights under this Agreement, the prevailing party shall be entitled to recover costs and attorneys' fees.

12.6 If any provision of this Agreement is held invalid or unenforceable by any court of competent jurisdiction, the other provisions of this Agreement will remain in full force and effect. Any provision of this Agreement held invalid or unenforceable only in part or degree will remain in full force and effect to the extent not held invalid or unenforceable. The parties agree to replace such void or unenforceable provision of this Agreement with a valid and enforceable provision that will achieve, to the extent possible, the economic, business and other purpose of such void or unenforceable provision.

12.7 This Agreement (including the Enrollment Confirmation and exhibits hereto) constitutes the parties' entire agreement by and between the parties with respect to the subject matter hereof and supersedes any prior or contemporaneous agreement or understanding by and among the parties with respect to such subject matter.

12.8 CYFLARE SECURITY is not responsible for any failures or delays in performing under the Certification Warranty that are due to events outside of CYFLARE SECURITY reasonable control. The Certification Warranty may not be available in all jurisdictions and is not available where prohibited by law or where not offered by CYFLARE SECURITY or by Provider.

12.9 The parties have agreed that this Agreement as well as any notice, document or instrument relating to it be drawn up in English only.

Schedule 2 (Exhibit B)

Certification Warranty Confirmation Summary*

Subject to all the terms and conditions in the Agreement, the Certification Warranty provides the following Certification Warranty Indemnification Levels:

Participants enrolled in the $500,000 Indemnification Level*

Certification Warranty Indemnification $500,000 Level	**Per Event**	**Per Participant**
Compliance Event	A Maximum of $100,000 USD	$100,000 USD
Ransomware Event & BEC Event	A Maximum of $100,000 USD	$100,000 USD
Cyber Legal Liability Event **	A Maximum of $250,000 USD	$250,000 USD
Business Income Event	A Maximum of $50,000 USD (*There is a $2,500 USD per-claim deductible that applies to this Event)*	$ 50,000 USD

Participants Enrolled in the $1,000,000 Indemnification Level*

Certification Warranty Indemnification $1,000,000 Level	**Per Event**	**Per Participant**
Compliance Event	A Maximum of $200,000 USD	$200,000 USD
Ransomware Event & BEC Event	A Maximum of $200,000 USD	$200,000 USD
Cyber Legal Liability Event **	A Maximum of $500,000 USD	$500,000 USD
Business Income Event	A Maximum of $100,000 USD (*There is a $2,500 USD per-claim deductible that applies to this Event)*	$100,000 USD

**Participant must first exhaust any other service warranty that would apply to these expenses.*

***Cyber Legal Liability/Media - Participant must exhaust all other financial benefits before triggering this Indemnification Level.*

The Indemnification Level, Per Event, and Per Participant amounts reflected in the tables above, although shown in USD, means the equivalent amount in the applicable foreign currency reflected within an Order Form.