OmniNet, Inc. Data Breach Limited Warranty

THIS LIMITED WARRANTY IS VALID ONLY IN THE UNITED STATES, CANADA, AND PUERTO RICO

OmniNet, Inc. will reimburse the **Warranty Holder** for **Warranty Holder Losses** resulting from a **Certified Computer Attack** or **Data Breach** in excess of any applicable deductible first occurring during the **Service Period** and reported to OmniNet pursuant to the terms of this **Data Breach Limited Warranty** (the "**Limited Warranty**") up to the maximum annual aggregate limit or sublimit applicable by coverage for the level of service selected by the **Warranty Holder** (the "**Claim Benefit**"). Refer to the Coverage Chart - Claim Benefit by Level of Service ("**Coverage Chart**") below for **Claim Benefit** limitations and the annual aggregate limit and sublimit by coverage applicable to the level of service purchased.

COVERAGE CHART – CLAIM BENEFIT BY LEVEL OF SERVICE**

	Service Level Options	
	Lite	Standard and Pro
Annual Aggregate Limit	$10,000	$100,000
Data Restoration Cost	$2,500 Sublimit per event	$30,000 Sublimit per event
Systems Restoration Cost	$2,500 Sublimit per event	$30,000 Sublimit per event
Customer Notification	$5,000 Sublimit per event	$15,000 Sublimit per event
Public Relations Expense	$2,000 Sublimit per event	$6,000 Sublimit per event
Re-creation of Data Cost	Not Included	$10,000 Sublimit per event
Consumer Monitoring	Not Included	$15,000 Sublimit per event
Forensics and/or Legal Review	Not Included	$5,000 Sublimit per event

The **Warranty Holder will be reimbursed only for ONE **Claim Benefit Occurrence** per **Warranty Holder** per twelve (12) month period during the **Service Period**.

I. DEDUCTIBLE AND WAITING PERIOD FOR COVERAGE

The **Claim Benefits** provided by this **Limited Warranty** (as listed in the chart above) are subject to a deductible of 10% of the annual aggregate limit per occurrence ("**Deductible**"). The **Limited Warranty** will have a waiting period of thirty (30) days. Such waiting period begins on the date following purchase that the **Warranty Holder** completes both (a) the setup of the subscription to the OmniNet security service AND (b) the warranty activation form ("**Subscription Date**"), and ends on the **Effective Date** of the OmniNet security service. There will be no reimbursement available for **Losses** that arise during the thirty (30) day waiting period.

II. DEFINITIONS

1. **Certified Computer Attack** means damage to **Warranty Holder's Computer System** or data arising from malicious code including viruses and worms, Trojans, spyware and keyloggers (collectively "**Malware**"), which results in copying, destruction or misappropriation of the **Warranty Holder's** customers' personally identifiable information. This does notmean damage from shortcomings or mistakes in legitimate electronic code or damage from code installed on the **Warranty Holder's Computer System** during the manufacturing process, and does not include damage arising from **Malware** that is propagated or forwarded in connection with hardware or software created, produced or modified by the **Warranty Holder** for sale, lease or license to third parties.

2. **Computer System** means computer hardware, software or firmware and data stored thereon, linked together through anetwork of two or more computers, or accessible through the Internet, including network infrastructure, input, output, processing, storage and off-line media libraries. **Computer System** also includes those written policies and procedures applicable to the security of a computer network.
3. **Consumer Monitoring** refers to the costs incurred by the **Warranty Holder** for providing one (1) year of credit monitoring services for **Warranty Holder's** customers if customer data was exposed due to a **Data Breach**.
4. **Customer Notification** refers to the actual cost incurred by the **Warranty Holder** for notifying its customers if customer data is exposed due to a **Data Breach**.
5. **Data Breach** means an occurrence during the **Service Period** which includes a single act or a series of related acts, whether committed by one or more persons, of theft of personally identifiable information or damage to data records and/or systems.
6. **Data Restoration Cost** refers to the actual costs incurred by the **Warranty Holder** for hiring a firm to restore data from electronic sources that was lost or corrupted due to a **Certified Computer Attack** or **Data Breach** on the **Warranty Holder's** system.
7. **Denial of Service Attack** or **Distributed Denial Service Attack** means an attack intended by the perpetrator to overwhelm the capacity of a **Computer System** by sending an excessive volume of electronic data to such **Computer System** in order to prevent authorized access to such **Computer System**.
8. **Effective Date** means thirty (30) days after **Purchase Date**, and will mark the beginning of the **Service Period**.
9. **Forensics Review** refers to actual costs incurred by the **Warranty Holder** for hiring a computer forensics professional for the purpose of determining the origination of a breach and to assess the damage done to **Warranty Holder's Computer Systems** and data.
10. **Legal Review** refers to actual costs incurred by the **Warranty Holder** for hiring an attorney who can provide guidance on how to best respond to a breach.
11. **Loss** or **Losses** mean the actual costs and expenses incurred by the **Warranty Holder** resulting from a **Certified Computer Attack** or **Data Breach** up to the maximum annual aggregate limit or sublimit applicable by coverage for the level of service selected by the **Warranty Holder**.
12. **Public Relations Expense** refers to the costs incurred by the **Warranty Holder** from hiring a public relations firm to help mitigate damages relating to **Warranty Holder's** response from a **Data Breach**.
13. **Occurrence** means an incident of an actual or attempted fraudulent, dishonest or criminal act or series of related acts, whether committed by one or more persons.
14. **Re-creation of Data Cost** refers to the actual costs incurred by the **Warranty Holder** for hiring a firm to recreate data using non-electronic sources that was lost or corrupted due to a **Certified Computer Attack** or **Data Breach** on the **Warranty Holder's** system.
15. **Service Period** is the period of time during which if the **Warranty Holder** incurs a **Loss**, such **Loss** will be eligible for reimbursement in accordance with the other terms and conditions of the **Limited Warranty**. The **Service Period** will begin on the **Effective Date** and will run so long as the **Warranty Holder** pays for the OmniNet security service. The **Service Period** ends on the **Termination Date**.
16. **System Restoration Cost** refers to the actual costs incurred by the **Warranty Holder** for hiring a firm to restore its **Computer Systems** to the functionality level it had prior to the **Certified Computer Attack** or **Data Breach** on its **Computer System**. This would include removing malicious code, correcting configuration of the system and reinstalling necessary software.
17. **Termination Date** means the same date upon which the **Limited Warranty** is cancelled or non-renewed, for example, due to non-payment, and marks the end of the **Service Period**. The **Warranty Holder** will not be eligible to receive reimbursement for **Losses** incurred on or after the **Termination Date**.
18. **Unauthorized Computer Access** means the gaining of access to a **Computer System** by an unauthorized person(s) or by an authorized person(s) in an unauthorized manner. **Unauthorized Computer Access** is not included in **Certified Computer Attack**.

19. **Unauthorized Computer Use** means the use of a **Computer System** by an unauthorized person(s) or by an authorized person(s) in an unauthorized manner. **Unauthorized Computer Use** is not included in **Certified Computer Attack**.
20. **Warranty Holder** means the purchaser of the OmniNet security service to whom OmniNet issues the **Limited Warranty**.

III. EXCLUSIONS TO THE LIMITED WARRANTY

OmniNet will not pay the **Warranty Holder** for any **Loss** caused directly or indirectly by any of the following. Such **Loss** is excluded regardless of any other cause or event that contributes concurrently or in any sequence to the **Loss**.

1. Loss to the internet or internet service provider, computer or **Computer System** not owned or leased by the **Warranty Holder** and operated under their control.
2. Any costs associated with researching or correcting any deficiencies.
3. Any fines or penalties.
4. Any criminal investigations or proceedings.
5. Any blackmail, threat or extortion. This includes, but is not limited to, ransom payments and private security assistance.
6. Intentional or willful complicity in a **Certified Computer Attack** or **Data Breach** by the **Warranty Holder**.
7. Any fraudulent, criminal, dishonest act, error or omission or any intentional violation of the law by the **Warranty Holder** or their employees, subcontractors, agents or assigns.
8. Any failure caused by outages or disruption of power, utility services, satellites, or telecommunications external services including but not limited to electrical disturbances, surge, brownout or blackout.
9. Any failure caused by bankruptcy, financial impairment, or insolvency.
10. Fire, smoke, explosion, lighting, wind, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, act of God, or any other physical event or peril.
11. Failure in design, architecture or configuration of the **Warranty Holder's Computer System**, including failure to design for traffic and capacity requirements.
12. Any **Loss** or circumstance the **Warranty Holder** previously provided notification of to a prior warranty or insurance provider.
13. Any strike, similar labor action, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not) civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular uprising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder, defend, control, prevent or suppress any of the foregoing.
14. Any **Loss** resulting from or arising out of the destruction, confiscation or seizure by order of any government or public authority.
15. Voluntary disclosure of any code or other security information which can be used to gain access to a **Warranty Holder's** account to someone who subsequently contributes to a **Data Breach**. This does not include disclosure of any code or other security information which can be used to gain access to a **Warranty Holder's Computer System** when the **Warranty Holder** is or was under duress.
16. Any **Loss** to any computer owned or leased by the **Warranty Holder** which occurs while such computer is removed or taken offline from the OmniNet security service (including the cloud protection service); nor any **Loss** as a result of such computer being removed or taken offline from the OmniNet security service (including the OmniNet cloud protection service).
17. Any **Loss** resulting from the failure to ensure that the **Computer System** is protected by the OmniNet security service (including the cloud protection service) at all times.
18. Any **Loss** occurring from ordinary wear and tear or gradual deterioration of the **Computer System** or digital assets.
19. Any violation of the Securities Exchange Act of 1933 as amended, the Securities Exchange Act of 1934, as amended, any state Blue Sky or Securities Law or rules, regulations or amendments issued in relation to such acts, or any similar state, federal or foreign states or regulations.

20. The propagation or forwarding of **Malware** in connection with hardware or software created, produced or modified by the **Warranty Holder** for sale, lease or license to third parties.
21. Any failure by the **Warranty Holder** to effect or maintain any insurance or bond.
22. Any breach resulting from a **Distributed Denial of Service Attack** or from a **Denial of Service Attack**.
23. Any breach to the OmniNet cloud platform and/or technology infrastructure.
24. Any breach due to the use of credit card skimmers, taking photos or credit cards, writing down numbers (any type of physical theft).
25. Any **Data Breach** due to the insertion of any external device into the computer.
26. If a request from OmniNet for remediation is not responded to within **48 hours** by the **Warranty Holder** then any claim arising from the lack of remediation in that time frame is not covered.
27. Any breach due to weak or stolen credentials.
28. Any **Loss** arising out of, based upon, or attributable to the infringement of copyright, patent, trademark, trade secret or other intellectual property rights.
29. Any actual or alleged violation of the Organized Crime Control Act of 1970 (commonly known as Racketeer Influenced and Corrupt Organizations Act or RICO), as amended, or any regulation promulgated thereunder or any similar federal law or legislation, or law or legislation of any state, province or other jurisdiction similar to the foregoing, whether such law is statutory, regulatory or common law.
30. Any **Loss** arising out of or resulting from any actual or alleged antitrust violation, restraint of trade, unfair competition, or false or deceptive or misleading advertising or violation of the Sherman Antitrust Act, the Clayton Act, or the Robinson-Patman Act.
31. Failure by the **Warranty Holder** to provide and maintain appropriate computer and internet security.
32. Failure of the **Warranty Holder** to provide and maintain appropriate physical security for their premises, **Computer Systems** and hard copy files.
33. Failure of the **Warranty Holder** to protect transactions such as credit card payments, debit card payments, and check payments.
34. Failure of the **Warranty Holder** to appropriately dispose of files containing personally identifiable information or personally sensitive information, including but not limited to, shredding hard copy files and destroying physical media used to store electronic data.
35. Failure by the **Warranty Holder** to provide and maintain daily off-site backup of **Computer Systems** in accordance with a written business continuity plan that is tested at regular intervals.

IV. LIMITATION OF LIABILITY AND DURATION OF WARRANTY

1. OmniNet shall not be liable to **Warranty Holder** for more than the annual aggregate limit or sublimit shown in the **Limited Warranty**. The annual aggregate limit is the most OmniNet will pay for **Losses** under this **Limited Warranty** for all coverages combined, regardless of the number of covered causes of loss, persons, or entities covered by this **Limited Warranty**, claimants, losses reported, or insuring agreements triggered.
2. Any sublimit shown in the **Limited Warranty** is part of, subject to, included within, and does not increase the **Limited Warranty Claim Benefit** aggregate limit.
3. The **Limited Warranty's** duration for each **Warranty Holder** will be concurrent with the **Service Period**. The **Warranty Holder** will **NOT** be reimbursed for any **Losses** arising on or after the **Termination Date** (as defined above).

V. IN THE EVENT OF A LOSS

The **Claim Benefits** described in the **Coverage Chart** above for this **Limited Warranty** are available only for **Losses**. In the event the **Warranty Holder** seeks to obtain any of the **Claim Benefits** described above, in connection with a **Loss**, the **Warranty Holder** shall:

1. Promptly, but no later than thirty (30) days after the discovery of a **Loss**: (a) notify OmniNet' Third Party Administrator (the "**TPA**") of the **Loss** by calling 1-800-972-0059; (b) submit to the TPA written proof of **Loss**; and (c) provide any other reasonable information or documentation the TPA may request, including but not limited to, estimates, quotes or paid invoices related to **Losses**.

2. Provide all assistance and cooperation the TPA may require to conduct its investigation of and to determine the extent of any **Losses** asserted by the **Warranty Holder**, including but not limited to: (a) Immediately forwarding to the TPA any notices, summons or legal papers received in connection with a **Loss**, **Certified Computer Attack**, or **Data Breach**; (b) Authorizing the TPA to obtain records and other information with regard to any **Loss**; and (c) Cooperating with and helping the TPA to enforce any legal rights the **Warranty Holder** or OmniNet may have against anyone who may be liable to them.
3. **Warranty Holders** may engage service providers prior to submitting claims to the TPA, however, **Warranty Holder** accepts the risk that any such services obtained prior to receiving formal approval from the TPA may not be reimbursable under the **Limited Warranty**.

VI. THE WARRANTY HOLDERS RIGHTS UNDER STATE LAW

This **Limited Warranty** provides the **Warranty Holder** specific legal rights, however, they may have other rights that vary from State to State.