Digimune

Cyber Warranty Terms & Conditions

Under these terms and conditions, the Digimune warranty guarantees the integrity of its cybersecurity products and the ability of these products to prevent cybercrime, fraud and identity theft against you, the end-user.

Subject to the terms and conditions below, you are protected against:

- **Hacking-Inflicted Device Damage**

  In the event that your electronic device is hacked during a cyberattack, we will provide technical support to rectify and restore your electronic device in terms of the Digimune Warranty Certificate.

  If we are unable to repair your device, we will replace it with a similar make and model in terms of the Digimune Warranty Certificate.

- **Cyber Extortion**

  In the event that you are a victim of a cyber extortion attack, we will provide you with technical support.

  If the attack can be stopped without paying the extortion amount, we will restore your electronic device in terms of Digimune Warranty Certificate.

  If it becomes apparent that the extortion amount needs to be paid to unlock your electronic device, we pay this amount in terms of the Digimune Warranty Certificate, subject to approval from us.

- **Loss of Funds**

  In the event that an unauthorised third party gains access to your protected device and obtains stored information on your lock-in credentials as a result of the failure of the Digimune cybersecurity software, which enables the hacker to cause financial loss to you, we will respond in terms of the Digimune Warranty Certificate.

  The onus lies with you to provide evidence that the stolen funds was caused by the failure of the Digimune protection software.

  Examples of stolen funds, where an unauthorised third party has obtained access to the device, by way of a hack, includes:
  - EFT / Online Banking Fraud, where the hacker either transfers funds remotely from the protected device or obtains security details from the protected device and makes EFTs using this information.

- Online Shopping Fraud, where the hacker either made purchases remotely from the protected device or obtained security details from the protected device and has made purchases using this information.

Definitions

- **We / Us / Our**
  Digimune group which concluded exclusive agreements with certain global cybersecurity product suppliers to provide this warranty cybersecurity software, products and services as outlined within these terms and conditions.

- **You / Your / Yours**
  The end-user (only a natural person who used his/her own personal or company-allocated digital system), who received the approved software from Digimune or service provider network.

- **Cybersecurity Software Product**
  Any approved product provided to you by Digimune or service provider network.

- **Digimune Warranty Certificate**
  The Certificate(s) annexed to this terms and conditions including any other Certificates which may, at any time hereafter be issued, whether in substitution for or in addition to the existing terms and conditions.

- **Digital System**
  Your digital system, including desktop, laptop, smartphone or other devices used by you to access your data, information or digital money.

- **Digital Identity**
  Your name, address, identification number, bank or credit card account number – any information relating to, or method of, your personal identification that is accessible online via a computer device on which Identicate software is installed.

- **Keys to Digital Identity**
  Include any online device security, such as a password, a passphrase, a Personal Identification Number (PIN), OTP (One time PIN), username, account number, or any other authentication method used to control, restrict and / or allow access to your money.

- **Hacking Incident**
  Any electronic attack of a malicious or unauthorised nature, initiated by a third party, with the intention or purpose of disrupting, disabling, damaging, destroying, altering, encrypting, overloading, or interfering with the device or software systems or records, or destroying the integrity of the data or stealing controlled information.

- **Digital Identity Theft**
  Includes, but is not limited to, the fraudulent use of your personal identity to establish credit accounts, secure loans, enter into contracts or commit crimes.

- **Cyber Extortion**
  A crime involving a hacking incident or threat, coupled with a demand for money or some other response in return for stopping or remediating the attack – via malicious activity, such as ransomware or distributed denial-of-service (DDoS) attacks, to steal data and threaten to expose it.

- **Money**
  Varying amounts of currency that is stored in a digital account and used for digital payments, e.g. credit / debit card payments, app payments, online songs, electronic funds transfer (EFT).

- **Financial Loss**
  Any loss where money was stolen as defined in this terms and conditions.
- **Funds Transfer**
  Online money transfer from the end-user to a third party account.

- **Bank**
  Any bank, savings, association, credit union, or any other person or business that directly holds your money. The bank typically issues keys to your digital identity (e.g. a PIN code) to access and enable online money transfers.

- **Cancellation Date**
  The date on which the warranty either lapses or is cancelled.

Specific Terms and Conditions

This warranty is solely applicable to our cybersecurity software products that were provided by us and installed on your device, by you, for the sole purpose of preventing cybercrime.

We guarantee the integrity of our cybersecurity products and the ability of these products to prevent cybercrime against yourself.

This warranty, at our option and discretion, may also to re-instate, repair, replace, negotiate, and pay on your behalf, or reimburse you for damage caused by a hacking incident or cyber extorsion event due to cybercrime, when the cybersecurity software products fail to prevent cybercrime, subject to the following terms and conditions:

- The approved cybersecurity software products provided to you are installed, with the latest update, and used in the appropriate manner, as per the operation manual; and

- If a company-allocated digital system was used, you must prove that your company device was installed with a licensed cybersecurity software product purchased from us, and that the product has been updated according to the manufacturer recommendations and instructions, at the time of the incident.

Exclusions

- If you are not a natural person.

- Where your digital operating system is not up to date or in line with the requirements of the version of the cybersecurity software products provided by us.

- Any loss due to the use of unlicensed software.

- Notifications of losses submitted after 31 days of the alleged hacking incident.

- Any form of financial loss, other than Loss of Funds as described in this warranty.

- Losses associated with interest, damages, third party claims, fees incurred, and other costs that may be a consequence of the alleged hacking incident or cyber extortion event.

- Losses suffered wherein you have deliberately or inadvertently shared or given your digital identity and / or “keys” (login details) to any third party, irrespective of the reason, including (but not limited to) phishing, vishing and splicing scams.

- In-store (e.g. shop) and other card transactions not originating from your digital system.

- Currencies or accounts such as the Bitcoin ledger or other crypto-currency ledgers, that store digital value, but are not a registered bank and regulated entity.

- When your government or quasi-government seizes claimants money for whatever reason (or as part of war-like acts and military uprisings, terrorist activities, or syndicated online fraud schemes).

- Losses associated wherein you committed an act of fraud, dishonesty, misrepresentation or any wilful act without or with a third party.

Compensation

Only in the event of our installed cybersecurity software failure, this warranty will act. You must provide us with evidence that you suffered a loss in terms of this warranty, and provide evidence that you have not been compensated for the loss.Yyou could never be compensated twice for the same event whilst this warranty is in force and valid.

Claim Procedure

- **Step 1: Inform Police**
  Inform the police immediately, within 24 hours, after the event that led to the loss. You will need to provide the police docket number when notifying us of the loss.

- **Step 2: Inform Us**
  Inform us, as soon as possible, of an incident that could lead to a loss, but within 31 days after the event. Give us all the relevant details. The warranty loss can be lodged electronically by going to: TBA

- **Step 3: Supply Supporting Information**
  If you haven’t already dealt with this when you first reported the loss, please ensure that you submit your warranty loss electronically within 31 days.

- **Step 4: Assist with Any Legal Proceedings**
  Your assistance will be required should we decide to start legal proceedings against any party responsible for the loss or damage. Note that any such legal action may be taken in your name.

- **Step 5: Sign Release**
  You may have to sign a release before we will compensate you

Unless we specifically offer to pay or make provision for payment, the entire procedure above is facilitated at your own expense.

General Terms and Conditions

- This warranty is for the worldwide use of your devices.
- This warranty is subject to the South African law. If any of the terms or conditions of this warranty is in breach of existing legislation, it will be amended, so as to comply with South African law.
- Only you as the registered end-user as described on the Digimune Warranty Certificate shall have access to this warranty. This warranty is non-transferable.
- You must ensure that all the information provided to us about yourself, and your risk profile, is true and accurate and updated regularly should it change.
- You must take reasonable steps to prevent any loss or damage, or we may not compensate you for any loss.
- Your subscription payments must reach us on time. All subscriptions are payable in advance, before the warranty incepts. During a period of non-payment of subscription, this warranty is not valid and becomes null and void.
- We reserve the right to cancel this warranty, with immediate effect, should we find any material facts that could influence/jeopardise our ability to provide cover under this warranty – such as misrepresentation or financial enrichment. We will give you 31 days written notice, if we want to change the conditions of this warranty.

Processing and Protection of Personal Information

Your privacy is of the utmost importance to us. We will take the necessary measures to ensure that all information, including personal information provided by you, or which is collected from you, is processed following the provisions of global standards and legislation and is stored safely and securely.

The information you provide to us will be stored on databases and shared with other parties in the industry to gather industry statistics, improve the quality of risk assessment, and combat fraudulent claims. It is important to understand that this information will remain at the disposal of these parties, even after your Benefit with us ends.

You accept that your personal information may be used for the following reasons:

- To establish and verify your identity in terms of the applicable Laws;
- To enable us to fulfil our obligations in terms of this warranty;
- To enable us to take the necessary measures to prevent any suspicious or fraudulent activity, in terms of the applicable Laws;
- Reporting to the relevant regulatory authority / body, in terms of the applicable Laws having jurisdiction.

We may share your information for further processing with the following third parties, which third parties must keep your personal information secure and confidential:

- Payment processing service providers, merchants, banks, and other persons that assist with the processing of your payment instructions;
- Law enforcement and fraud prevention agencies and other persons tasked with the prevention and prosecution of crime;
- Regulatory authorities, industry ombudsmen, governmental departments, local and international tax authorities, and other persons that we, following the applicable Laws, are required to share your personal information with;
- Our service providers, agents and subcontractors that we have contracted with to offer and provide products and services to any customer in respect of this warranty; and
- Persons to whom we cede our rights or delegate our authority to in terms of this warranty.

You acknowledge that any personal information supplied to us, in terms of this warranty, is provided according to the applicable Laws and at your free will. Unless consented to by yourself, we will not sell, exchange, transfer, rent or otherwise make available your personal information to any other parties and you indemnify us from any claims resulting from disclosures made with your consent.

You understand that if we have utilised your personal information contrary to the applicable Laws, you have the right to lodge a complaint with us within ten days. Should we not resolve the complaint to your satisfaction, you have the right to escalate the complaint to the particular Information Regulator having jurisdiction.

For any queries relating to this document please contact us at: legal@digimunegroup.com