WARRANTY TERMS AND CONDITIONS

Definitions:
In this part of the software purchase agreement (the Warranty), the following expressions shall have the following meanings:

1. Software - DynaRisk and Kaspersky products sold to the End User by Cybercare4U.
2. End User – the customer who has purchased DynaRisk and Kaspersky products from Cybercare4U through its Distributor. Throughout the Warranty we will refer to the End User as “You” / “Your” / “End User”
3. Financial Loss - the value of the Money stolen.
4. Keys to Your Digital Identity - include any online device security, such as a password, a passphrase, a Personal Identification Number (PIN), OTP (One time PIN), user name, account number or any other authentication method uses to control and/or restrict and or allow access to End Users Money.
5. Money – varying amounts of currency that is stored in a digital account and used for digital payments (e.g. app payments, songs on-line, credit or debit card, electronic Funds Transfer (EFT). The warranty intends to only make good losses in funds stolen due to a breach in the Software.
6. Fund Transfer – online Money transfer from End User to 3rd party accounts on-line.
7. Bank - any bank, savings, association, credit union, or any other person or business that directly holds End User’s Money. The Bank typically issues Keys to Digital identity to End Users (e.g. a PIN code) to access and/or enable Fund transfers.
8. Digital Identity –End User’s name, address, identification number, bank or credit card account number, any other information relating to personal identification, any other method of End User identification that is accessible online via a computer device on which Cybercare4U Software is installed. Your Digital Identity does not relate to the theft of, say, Your ID number where Your physical ID card was stolen. For the avoidance of doubt, the Warranty intends to make good losses, up to a limit, due to a security breach of the Software You purchased from us, and not where the Keys to gain access to Your Digital Identity was surrendered in any other manner.
9. Digital Identity Theft - is limited to the fraudulent use of End User’s Digital Identity to establish credit accounts, secure loans, enter into contracts or commit crimes. The information used in the stolen identity event varies (e.g. End User name, address, identification number, bank or credit card account number, personal identification information or other method of End User identification).
10. Digital System –End Users digital system including desktop, laptop, smart phone and other devices used by End User to access their Money.

Warranty:

The Warranty is solely applicable to cyber-security Software products DynaRisk and Kaspersky sold to the End User by Cybercare4U for the purpose of prevention of cyber-crime.

Under the terms of this Warranty Cybercare4U guarantees the integrity of the Software and the ability of the Software to prevent cyber-crime, fraud and Digital Identity Theft against the End User. The warranty further commits to reimburse personal Financial Loss due to cyber-crime against the End User subject to the following terms and conditions:

1. The Software sold to You is used in the appropriate manner and in accordance with the terms and conditions of the warranty.
2. You respond to warning messages provided by the Software, such as a notification stating that Your Digital Identity has been compromised. You will be required to update all the Keys to Your Digital Identity such as passwords and personal identification numbers (PIN’s) in these circumstances. To the extent that You do not update Your passwords and PINs that is attached to your Digital Identity, the Warranty will not pay out as the Software was not breached.

3. In the event that the Software, when used as specified, fails to prevent cyber-crime, fraud caused by Digital Identity Theft and the End User suffers Financial Loss, then the Cybercare4U Warranty will apply and Cybercare4U will compensate the End User for claims made according to the terms set out in (4) below.

4. Compensation:

   4.1. Where approved by Cybercare4U, the warranty payment will be paid to the person who purchased the Software (the person that contracted with Cybercare4U (“Contracting party”), and not any other person or entity, irrespective of the computerised device that has the Software product installed. This also means that if you give your devices to another person and your or their details are stolen from that device, the warranty due to a Software security breach would not respond.

   4.2. The claims process:

   4.2.1. Contact Cybercare4U, and submit a claim for a refund within 30 days of discovering that Money or Digital Identity has been stolen or within 180 days of the date of actual Financial Loss, whichever is earlier. You also need to notify us of incidents where a future claim is anticipated (e.g. where you suspect that your Digital Identity was stolen which could lead to Financial Loss; prompt notification enables us to make sure that the circumstances that led to Money being stolen qualifies for the Warranty Payment. To avoid doubt, if there is an event that took place that you think may lead to the loss of Money, you need to let us know;

   4.2.2. Inform the Bank to check and verify the Financial Loss due to a Digital Identity Theft event that occurred and provide proof of notification to the Bank to Cybercare4U;

   4.2.3. Inform the police / authorities of the Financial Loss due to a Digital Identity Theft event as soon as possible, but no later than 24 (twenty-four) hours after becoming aware of the event;

   4.2.4. We may log on to Your computer using remote Software to verify the Software on Your computer and research the circumstances around the alleged Financial Loss due to a Digital Identity Theft. You hereby consent that you will provide us access to you devices linked to the Software and waive Your rights to privacy insofar as we need access to Your computer/device in order to verify details around the alleged breach of the Software acquired from us.

   4.2.5. Cybercare4U will request documentation to verify that Money has been stolen. Any cost associated with obtaining the required documentation will not be covered by us. All reasonable information and documentation we ask from You must be provided within the timeframe we set. The documentation needed includes, but is not limited to, the following:

   4.2.5.1. The police report;
   4.2.5.2. The police case number and name and contact details of investigating officer;
   4.2.5.3. Bank statement for validation of transaction;
   4.2.5.4. A letter from the Bank stating that they will not reimburse the Financial Loss incurred;
   4.2.5.5. Evidence that End User has complied with the requirements for the latest version of Software on the device. This would entail a screen shot of Your Kaspersky security Software and Your operating system, and what Your latest Software and operating system version is and when it was last updated.
4.2.5.6. Should any further verification need to take place, Cybercare4U will need to check the infected device or the device that the incident took place on.

The process will be as follows -

4.2.5.6.1. Cybercare4U will send a digital indemnity and consent form to End User to allow access to the affected device. Cybercare4U technical team will then access the problematic device and investigate.

4.2.5.6.2. A digital forensic tool is used, which gathers information about the operating system and hardware component, to generate a report of affected systems. The forensic tool simply scans the backend of the system for any incompatibilities and points out the breach point and any issues which may have arisen from this, including outdated drivers, incompatible Software etc.

4.2.5.6.3. The technical team then advises End User on steps to take to resolve issues found on the system and how to further protect the device.

4.2.5.6.4. Depending on the outcome of investigation the Warranty will make good the Financial Loss up to the agreed limit of the Warranty.

4.2.6. Inform Cybercare4U in the event of or awareness of any possible prosecution, legal proceedings or claim that could be lodged against the End User as a result of the same incident during or since their claim to us.

4.3. The Warranty will only be paid against personal Financial Loss only and will be paid within 30 days of approval by Cybercare4U verifying that the Warranty was breached.

4.4. The Warranty covers a MAXIMUM amount of R40 000 per annum (counted from the date of purchase or renewal of licenses to the Software product) and will only be paid where there was a Financial Loss verified by Cybercare4U.

4.5. The Warranty will only be paid to person that purchased the Software from us and who can prove that the computerised device storing their Digital Identity was loaded with our Software and the failure of our Software contributed in some way in the stealing of their Digital Identity.

5. Please note our Warranty includes the following, subject to You using the Software in accordance to the prescriptions set out under the heading “Warranty”, as set out above:

5.1. Fraudulent Online Purchases – When neither You or Your actual credit card are present at the point of sale

5.2. Fraudulent In-App Purchases – When Your credit card details are used to pay for mobile applications not authorised by Yourself

5.3. Phishing Scams - Fraudsters con You into providing Your personal information and use it to perpetrate fraud

5.4. Virus Attacks - Malware or viruses unwittingly downloaded on Your computer or device that harvest Your personal data

5.5. Fraudulent EFT’s - Someone gains access to Your banking details by computerised means and transfers money from Your account without Your knowledge.

6. Please note our Warranty excludes the following:

6.1. Claims submitted after 30 days of discovery of the alleged Financial Loss or 180 days after actual Financial Loss, whichever is the earlier date.

6.2. Claims for interest, damages, 3rd party claims, fees incurred and other costs that may be a consequence of the alleged Financial Loss.

6.3. Claims found to be fraudulent or where the End User has attempted to derive financial benefit or where the Financial Loss was recovered from a 3rd party.
6.4. Claims made where the End User has deliberately or inadvertently shared or given their Digital Identity and/or Keys to Digital Identity to any third party irrespective of the reason.
6.5. Claims where DynaRisk and Kaspersky Software have been purchased from vendors other than Cybercare4U.
6.6. In-store purchases (e.g. shop) that lead to a theft of the End User’s Digital Identity.
6.7. Cash transactions.
6.8. Currencies or accounts such as the Bitcoin ledger or other crypto-currency ledgers that store digital value but are not a Bank.
6.9. When End-User’s government or quasi government takes claimants Money for whatever reason (or as part of war-like acts and military uprisings, terrorists activities or syndicated online fraud schemes);
6.10. Any claim against loss due to use of unlicensed Software, computer viruses or similar destructive media introduced onto Your device for use of unlicensed Software.
6.11. Where End User’s device operating system is not up to date or in line with the requirements of the version of the Software purchased from Cybercare4U.
6.12. Where we need access to the device to verify if the Software breach and the End User fails to provide access.

7. Term of Warranty agreement
7.1. This Warranty is valid for 12 months from the date of purchase or latest upgrade of the Software by the End User.
7.2. This Warranty is automatically renewed for 12 months from the date of renewal and payment of the End User product Software licence agreement.

8. Good faith
8.1. This Warranty is given on the premise that all information provided is true and complete and that premise applies to any other party that may act on behalf of the End User. Cybercare4U acts on the information provided, therefore any information which is misleading, incorrect or false will prejudice warranty adjudication and/or compensation Pay-out.

9. Confidentiality
9.1. Cybercare4U respects the confidentiality of personal and End User information and will never misuse it.
9.2. Cybercare4U, Kaspersky and DynaRisk will never share any information with any entity, natural person or third party unless we are provided with written permission to do so, other than enabling Cybercare4U to perform its duties in this agreement.
9.3. The End User, agrees that Cybercare4U can access any relevant personal information and share it with the specialists they employ to determine if the warranty has failed due to breach in the Software and thus if your claim for Financial Loss is valid and may be approved for a warranty payment.