

**SALES LITERATURE – STAND-ALONE OWN DAMAGE PRIVATE CAR
INSURANCE POLICY**

UIN - IRDAN115RP0001V03201920

Scope of cover

Add-on Cover

Cyber Risk Cover

UIN: IRDAN115RP0001V03201920/A0183V01202627

In consideration of the payment of an additional premium by the Insured, as stated in the policy schedule, it is hereby agreed and declared that, notwithstanding anything to the contrary contained under this Add-On, the Company undertakes to indemnify the Insured against damage to or liability arising out of or in connection with a cyber-incident.

The Company's maximum liability under this add-on shall be limited to the Sum insured mentioned in the policy schedule or respective sub limits for the features as applicable.

This add-on provides coverage to the Insured against cyber-incident i.e vehicle unauthorized access, hacking, or any form of digital compromise, resulting in access impairment, misappropriation of funds, or legal liabilities.

Notwithstanding the foregoing, this Add-on shall only be operative where the Cyber Incident arises directly from or is connected to the Insured Vehicle's systems or integrated connected devices and provided that the Insured has exercised reasonable cybersecurity measures, including but not limited to the timely installation of all applicable software updates.

What's covered:

1. Restoring Vehicle Access

In the event that the electronic remote access systems of the Insured Vehicle—including but not limited to keyless entry systems, mobile applications, Bluetooth connectivity, or biometric authentication, are compromised due to a Cyber Incident, the Company shall indemnify the Insured for the costs incurred towards repair, reset, reinstallation, or restoration of the affected software or digital systems.

2. Cyber Extortion

The Company shall indemnify the Insured for any cost and expenses incurred due to an unauthorized access caused by a cyber-incident affecting systems installed in, or embedded within, or connected with the Insured's vehicle resulting to a cyber extortion.

Further, in cases where the Company requests Insured to notify any concerned authorities about the cyber extortion, same should be duly followed & complied with. Insured must notify any relevant concerned authorities of the cyber extortion.

3. Protection from Theft of Funds

The Company will indemnify the Insured for any direct and pure financial loss arising from unauthorized access caused by a cyber-incident affecting systems installed in, embedded within, or connected to the Insured's vehicle; such as syncing a mobile device, using connected vehicle controls via smartphone or tablet, resulting in theft of funds from the Insured's bank account, credit/debit card, mobile wallet, or other digital platforms, subject to policy terms and conditions.

Any claim admissible exclusively under this feature without any involvement of Own Damage(OD) or Vehicle Theft Claim shall not impact the No Claim Bonus (NCB) eligibility under the Policy.

4. Legal Costs if Someone Sues Insured

The Company will indemnify the Insured towards a legal liability due to unauthorized access caused by a cyber-incident affecting systems installed in, or embedded within, or connected with the Insured's vehicle resulting in a claim, suit, or proceeding instituted by a third party in connection with a data breach involving such third party's confidential information or personal data. The Company shall reimburse the Insured for reasonable and necessary legal expenses incurred in the defense of any such claim, provided that such expenses are incurred with the Company's prior written consent.

5. Your Legal Action Against Others (Data Breach)

In the event the Insured suffers a financial loss due to unauthorized access, misuse, or mishandling of Insured's personal or confidential data, relating to the Insured Vehicle, by any third party, the Company shall indemnify the Insured for reasonable legal expenses incurred in initiating legal proceedings against such third party for recovery of damages.

What's not covered:

This add-on shall not cover:

- Incidents not directly caused by or linked to a cyber-incident
- Events Insured already knew about before buying this cover
- Insured intentional or reckless actions
- Physical damage to the vehicle or regular wear and tear
- Investment or trading losses
- Physical or mental health issues arising out of the cyber-incident

- Loss/theft of intellectual property (like trademarks, patents)
- Claims between co-owners under the same policy (in case of Motor Floater Add-on)
- Improvements to Insured personal device beyond restoring it
- Gambling losses
- Cyber terrorism or war-related incidents
- Not updating Insured vehicle software or security patches as required by the manufacturer.
- Data stored in third-party apps not approved by Insured vehicle company.
- Server-level hacks, including but not limited to OEMs, OES or any server beyond control of the Insured.
- Any loss or consequential losses arising due to misplacement, destruction, modification, unavailability, inaccessibility of and/or delay in trading with cryptocurrencies, consisting of coins (eg. Bitcoin, Ethereum, Ripple, IOTA), tokens (Eg. EOS, Nem, Tether) or public and/or private keys being used in conjunction with the aforementioned.
- Any loss or consequential losses arising in cases of failure to update the previous two versions of the software provided by the manufacturer shall be excluded from coverage.

Key terms applicable to all of the above coverages are defined below:

- **Compromise:** Any unauthorized control or access to Insured vehicle's digital systems.
- **Confidential Information:** Sensitive personal data not meant to be shared publicly.
- **Cyber-attack:** A targeted attack when someone uses computers or the internet to break into Insured vehicle & connected devices, with an intention to steal information, or cause damage.
- **Cyber Extortion:** Threats to deny entry, exit, use of the vehicle or damage to the vehicle or it's systems unless payment is made in the form of cash, marketable goods and services.
- **Cyber incident:** Any malicious act or malware including cyber-attack occurring on Insured vehicle and connected devices.
- **Data Breach:** Unauthorized access to or leak of Insured personal or confidential information.
- **Legal Costs/Expense:** Expenses for hiring lawyers, consultants, and court-related fees.

- **Malware:** Harmful software like viruses, spyware, ransomware, etc.
- **Personal Data:** means any data about an individual who is identifiable by or in relation to such data.
- **Theft of Funds:** Money stolen via unauthorized electronic transfer.
- **Third Party:** Anyone other than Insured (the policyholder).
- **Unauthorised Access:** shall mean unauthorised acquisition, duplication, manipulation, or disabling of any digital or electronic system used to control access to, unlock, start, or operate the insured vehicle.

CANCELLATION

The policyholder can cancel the policy at any time during the term, by informing the insurer. In case the Policyholder cancels the policy, he/ she is not required to give reasons for cancellation. In such case of cancellation, the insurer will refund proportional premium for unexpired policy period, if the term of the policy is upto one year and there is no claim(s) made during the policy period. In case the term of the policy is more than 12 months, the insurer will refund premium for the unexpired policy period, in respect of policy with the term more than one year and the risk coverage for such policy years has not commenced. The insurer can cancel the policy only on the grounds of established fraud, by giving minimum notice of 7 days to the retail policyholder.

GRIEVANCE CLAUSE

For resolution of any query or grievance, Insured may contact the respective branch office of the Company or may call toll free no.1800-2666 or may approach us at the sub section "Grievance Redressal" on our website www.icicilombard.com (Customer Support section). However, if the resolution provided by us is not satisfactory you may approach Insurance Regulatory and Development Authority (IRDA) through the Bima Bharosa Portal - <https://bimabharosa.irdai.gov.in/> or IRDA Grievance Call Centre(IGCC) at their toll free no. 1800 4254 732 / 155255. You may also approach Insurance Ombudsman, subject to vested jurisdiction, for the redressal of grievance. Details of Insurance Ombudsman offices are available at IRDA website: <https://irdai.gov.in/>, or on the Company's website at www.icicilombard.com or on <https://www.cioins.co.in/Ombudsman>.

STATUTORY WARNING PROHIBITION OF REBATES (Under Section 41 of Insurance Act, 1938)

(1) No person shall allow or offer to allow, either directly or indirectly, as an inducement to any person to [take out or renew or continue] an insurance in respect of any kind of risk relating to lives or property in India, any rebate of the whole or part of the commission payable or any rebate of the premium shown on the policy, nor shall any person taking out

or renewing [or continuing] a policy accept any rebate, except such rebate as may be allowed in accordance with the published prospectuses or tables of the insurer:

[Provided that acceptance by an insurance agent of commission in connection with a policy of any class of insurance business taken out by himself in relation to risks associated with his own life, health or property shall not be deemed to be acceptance of a rebate of premium within the meaning of this sub-section if at the time of such acceptance the insurance agent satisfies the prescribed conditions establishing that he is a bona fide insurance agent employed by the insurer.]

(2) Any person making default in complying with the provisions of this section shall be liable for a penalty which may extend to ten lakh rupees.