



Product: Personal Cyber

Manufacturer Information

Product information

To offer indemnity to individuals, and individual beneficiaries within a Group Policy arrangement, when their information security processes fail as a result of a cyber attack, phishing or ransomware demand.

Cybercrime targeting consumers is rapidly increasing, and this product aims to offer a degree of certainty in the event of a cyber related incidents including identity theft, ransomware, cyber attack, cybercrime, and smart device attack. This wide range of cover will effectively protect consumers from the threat of cyber criminals whilst reducing the impact to individuals in the event of a loss. Finally, an objective of this product is to provide a high standard of care to individuals purchasing cover.

Providing customer with access to cyber helplines shows customer interest is at the forefront of this offering. Insureds will be given access to the CyberScout incident hotline under their cyber policy. This provides the insured with a phone number, accessible 24/7, to call in the event of an incident. Professionals will then advise the customer of the appropriate next steps to aid in reducing the impacts of the incident, as well as reducing the risk of further events.

Core Cover:

- Cyber-attack - Costs incurred as a direct result of a cyber-attack by a hacker including:
 - Restoration of computers system
 - Replacement of computer system where economical restoration was not possible
 - Retrieval and restoration of data to the computer system
- Extortion - recovery costs or ransom payment if a hacker holds the insured party to ransom or threatens to reveal sensitive data, introduce malicious software, or create additional damage or destruction until a ransom is paid
- Identity Theft – Access to the cyber helpline and the services of a fraud specialist as well as additional costs including but not limited to credit monitoring.
- Cyber Crime – costs to replace personal documents incurred solely as a result of either credit card fraud or a phishing attack.
- Smart Devices and Wearables – restoration of connected home devices to condition prior to the cyber-attack.

Target market

This product is suitable for private individuals that are at risk of being victims of cyber crime or identity theft, outside of the UK or EEA. This also extends to group policies with individual beneficiaries that may be purchased in the name of a commercial entity.

The product can be sold as an add-on to household insurance, or may be sold on a standalone basis with tailored limits for high net worth individuals depending on the customer's specific insurance needs.

Types of customer for whom the product would be unsuitable

This product would not be suitable for commercial entities (with the exception of group policies with individual beneficiaries), or any individuals not at risk of the core covers of cyber crime or identity theft.

This product may be less suitable for individuals engaged in a trade, business or profession operated from their home where a separate commercial cyber insurance policy may be required to cover activities undertaken that relate to a trade, business or profession.

Product not to be sold in the UK or EEA.

**Any notable exclusions or circumstances where the product will not respond****Limitations:**

- Consultation with the Cyber Helpline required prior to making a claim.
- Incidents to be reported no later than 15 days after discovery by the insured.
- Insured to ensure that original data is backed up at least every 30 days and where there is service contract the terms of service between the insured and the service provider allow for data to be backed up.
- Passwords must be changed from the default password.
- Computer system must have anti-virus software installed.

Exclusions include but not limited to:

- Bodily injury
- Any loss that relates to or is used for the purpose of the insured's trade, business or profession or any other capacity other than the insured's personal capacity.
- Any liability arising from your connected home device
- Ransomware monies surrendered in a face-to-face encounter
- Amounts owed to a third party for damages fines or penalties.
- Any monies that are reimbursable from the insured's credit card company, bank or other financial institution.
- Costs to defend or institute legal proceedings
- Loss of internet connection.
- Property damage
- Theft of any possessions including when credit cards have been physically stolen

Limits of Liability:

- Stated in the schedule & policy documentation.

Excesses

- Deductibles stated in the schedule.

Other information which may be relevant to distributors

This product is permitted for sale with up to 4 distributors in the chain.

The product may be sold as:

- a stand-alone product;
- an add-on to another product such as home insurance; or
- as part of group employee benefit package

No further distributors in the chain are permitted without TMKS' approval. Any such approval will include consideration of their impact on product value.

Where Distributor 1 sells this Product via multiple other distributors (via sub-delegation or sub-brokering), it is their responsibility to ensure all distributors have been provided this document, have reviewed it and understand the content. If there is any additional remuneration, including commissions, fees or other 'non-standard' remuneration charged to the customer by other distributors, it is the responsibility of Distributor 1 to inform TMK of these details accurately and in full.

This product can be sold with or without advice in line with FCA regulations or local regulations if distributor is not regulated by the FCA.

All distributors are expected to fully understand the eligibility criteria, covers and exclusions of the product.

Sales journeys must identify customer eligibility and ensure that key information and choices to be made are presented to customers in a way that supports a customer through the process of understanding core cover and configuring optional elements of insurance to suit their specific demands and needs.



When a Group Policy is sold, the distributor should ensure that appropriate confirmation and details of cover purchased is provided to the individual beneficiaries under the policy. This also is to include details of how to make a claim & complaint. It is good practice for the customer documentation to set out all the terms and conditions relevant to the coverage, so the customer has everything they need to understand the cover they are receiving.

This product can be sold face to face, via telephone, online rating engine or electronic communication or a mix of these methods, as long as customers are provided with sufficient information to make an informed decision regarding the suitability of the product.

Commission & Fees

If there is a coverholder in the chain, they are expected to ensure that maximum commission rates do not exceed those stipulated within the Binding Authority Agreement.

The coverholder is expected to maintain oversight of all broker commissions (where applicable) and, where there may be a risk to product value, remedial action should be taken immediately including notification to Tokio Marine Kiln.

Brokers are reminded of their own regulatory obligations in relation to remuneration under PROD 4.3.6 as well as the requirements to make all necessary disclosures to the customer.

Where there are any fees charged by any member of the distribution chain these should be:

- commensurate with the service provided by the distribution.
- not have an adverse impact on customer value; and
- the distributor should ensure that TMKS is made aware of the fee amount and/ or method of calculation.

How value is assessed

Value is assessed based on a number of metrics, including underwriting, claims and complaints information as well as through broker and coverholder engagement.

Remuneration paid as set out in our agreements with distributors has been considered as part of the value assessment.

If additional add-ons (including premium finance) are sold alongside this product or additional remuneration is charged, this may affect the value for the customer.

Further information on our product approval processes can be obtained on request.

Date Product Review completed	August 2023
Expected date of next assessment	August 2024