



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 CyberClan 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:

- Device and Data Requirement - Costs incurred as a direct result of a cyber attack by a hacker including:
 - Restoration of computer 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 – personal financial loss as a result of triggers such as credit card fraud, social engineering fraud, and online shopping fraud.
- Cyber Bullying - costs arising from cyber bullying committed against the Insured, including forensic analysis, counselling services and lost wages.

Target market

The Personal Cyber product is specifically designed for private individuals and individual beneficiaries under group policy arrangements who seek protection against personal cyber risks. It targets customers who value comprehensive cover for cybercrime and identity theft, along with access to expert incident response services. Key characteristics include:

(1) Customer Profile:

- Primary Audience: Private individuals exposed to risks such as cyber-attacks, phishing, ransomware, and identity theft.
- Extended Audience: Individual beneficiaries under group policies purchased by employers as an employee benefit.
- High Net Worth (HNW) Individuals: Tailored limits available for customers requiring enhanced protection.

(2) Insurance Profile:

- Sold as:
 - (a) Standalone policy for individuals, including HNW customers.
 - (b) Add-on to household insurance policies where sold as an option opt-in add-on.
 - (c) Employee benefit under group policy arrangements.
- Policy duration: Up to 18 months (longer than standard 12-month term).



- (3) Customer Needs & Behaviours:
- Customers likely to value:
 - (a) expert support via incident hotline for immediate guidance during cyber incidents, including via Cyberclan
 - (b) Comprehensive protection against financial harm caused by cybercrime.
 - Typical behaviours:
 - (a) Concerned about increasing cyber threats and identity theft.
 - (b) Seeking peace of mind and proactive assistance in mitigating cyber risks.

- (4) Geographic Scope:
- Distributed outside the UK (product not authorised for sale in UK).

- (5) Distribution Channel:
- Sold through coverholders and brokers, via both advised and non-advised processes.
 - Channels include:
 - (a) Third-party online systems.
 - (b) Telephone and face-to-face interactions.
 - (c) Electronic communications.

- (6) Circumstances Where Product Delivers Greatest Value:
- Following incidents of:
 - (a) Cyber-attacks causing system/data loss.
 - (b) Ransomware demands or extortion threats.
 - (c) Identity theft requiring fraud specialist intervention.
 - Situations where immediate expert advice and technical support can reduce financial and emotional impact.

This product appeals to customers seeking certainty, expert guidance, and rapid response in the event of personal cyber incidents, particularly those who lack technical expertise or resources to manage such risks independently.

Types of customer for whom the product would be unsuitable

The Personal Cyber product is not appropriate for:

- (1) Commercial Entities
 - Businesses or organisations seeking cyber protection for trade, business, or professional activities.
 - Exceptions apply only where the policy is structured as a group policy with individual beneficiaries.
- (2) Individuals Outside the Core Risk Profile
 - Customers who are not exposed to personal cyber risks, such as identity theft, phishing, ransomware, or smart device compromise.
 - Individuals who already have comprehensive cyber protection under another policy.
- (3) UK Residents
 - The product is not approved for distribution in the UK, so customers domiciled there are excluded.
- (4) Customers Unable to Meet Minimum Security Requirements
 - Those unwilling or unable to maintain basic cyber hygiene, such as:
 - (a) Regular data backups.
 - (b) Changing default passwords.
 - (c) Installing antivirus software.

Any notable exclusions or circumstances where the product will not respond

Limitations:

- Consultation with the Cyber Helpline prior to making a claim.
- Incidents to be reported no later than 15 days after discovery by the insured.
- Insured to maintain cyber hygiene, which may include installing updates on devices, regular data back-ups, changing default passwords and installing anti-virus software.

Exclusions included 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 monies that are reimbursable from the insured's credit card company, bank or other financial institution.
- Infrastructure failure
- Property damage
- Theft of any possessions including when credit cards have been physically stolen.
- Unlicensed use of Data and software
- Misconduct
- Prior knowledge or notification

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.

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.

Where Distributor 1 sells this Product via multiple other distributors (via sub-delegation or sub-broking), 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.

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.

Total acquisition costs, defined as the aggregate of all commissions, brokerage and fees deducted from the customer's premium across the entire distribution chain before the premium reaches TMK as net premium, must not be equal to or exceed 50% without prior and explicit agreement of TMK.

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	March 2026
Expected date of next assessment	March 2027