Product: Cyber Affinity Schemes

Manufacturer Information

Product information

The product provides indemnity to individuals and eligible commercial entities as part of an affinity insurance programme, when their information security processes fail as a result of a cyber attack, phishing or ransomware demand.

The product has been designed to be sold to larger commercial entities, charities or affinity groups such as a trade association who in turn can add value to their customers/ members by offering their members/ customers an insurance solution that is designed purposely around their interests

The cover provided will vary depending on the approved affinity scheme and customer type. Cover may be provided to individual customers, individual beneficiaries under group arrangements and approved commercial affinity scheme participants, subject to the applicable policy wording, limits, exclusions and conditions.

Core Cover for personal:

- Cyber-attack - Costs incurred as a direct result of a cyber attack including restoration and/or replacement of computer system and/or the retrieval and restoration of data on the computer system
- Extortion - recovery costs and/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 – credit monitoring for the insureds.

Core Cover for commercial:

- Security and Privacy Liability damages and defence costs as a result of a claim arising from a security breach or privacy breach.
- Business Interruption Financial loss arising from privacy breach, security breach, or system failure impacting the insured's computer system.
- Digital Asset Destruction of data, computer programmes and electronic documents incurred as a direct result of a privacy breach, security breach, or system failure.
- Cyber Extortion expenses and ransom demand payments to avoid a privacy or security breach incurred directly as a result of a cyber extortion threat.
- Incident Response Expenses incurred as a result of a privacy breach or security breach.
- Cyber helplines and breach response services

Depending upon whether the scheme is intended for individual or commercial customers, optional coverage may include:

<u>Individual customers:</u>

- **Cyber Crime** – reimbursement for an insured's financial loss following scams such as phishing and/or credit card fraud.
- **Smart Devices and Wearables** – restoration of connected home devices to condition prior to the cyber-attack.
- **Online Shopping Fraud** - Fake or fraudulent website created by a third party to induce an insured into purchasing goods that will never be delivered
- **Cyber Bullying** - Two or more similar acts of harassment, including defamation of character, invasion of privacy, or threats of violence that are committed to an insured via a connected home device
- **Cyber Stalking** - Malicious use of your computer system to stalk, abuse or control you as evidenced by unwanted and persistent tracking of your whereabouts, monitoring your activities with threatening effect
- **Homeworkers Extension** - Security breach of your home business. This includes but is not limited to malware attacks, cyber extortion threat or identity theft.

<u>Commercial customers</u>:

- Regulatory Fines and Penalties and Defence Expenses as a result of a claim arising from a Security Breach or Privacy Breach.
- Multimedia Liability damages and defence expenses as a result of a claim arising from multimedia activities.
- Payment Card Industry Fines, Assessments and Expenses as a result of a Claim arising from a Security Breach or Privacy Breach.
- Contingent Business Interruption Financial arising from privacy breach, security breach or system failure impacting the insured's outsource service providers computer system.
- Reputational Harm Financial loss and crisis management costs incurred as a result of an adverse media event arising from a privacy breach, security breach or administrative error.
- Loss of Funds incurred directly as a result of a hack of the insured's computer System.
- Physical Damage following cyber-attack
- Cyber Crime / Social Engineering
- Non-Tech Contingent Business Interruption
- Incident Response (outside of the limit)

It is noted that each optional additional extras will be subject to their own clauses, conditions, limits and exclusions.

Target market

The product is designed for:

- individual customers receiving personal cyber insurance through an approved affinity, membership, employee benefit or embedded insurance arrangement; and
- eligible commercial entities, principally micro-enterprises, small businesses and permitted mid-commercial entities, obtaining cyber insurance through an approved affinity, association, group purchasing or membership arrangement.

Individual customers may receive cover as policyholders, insured members or beneficiaries under an approved affinity arrangement. The product is intended to address personal cyber exposures including fraud, identity theft, ransomware, data loss and attacks affecting personal systems or connected devices.

Commercial customers will ordinarily share identifiable characteristics, activities, membership relationships or cyber exposures that make collective distribution appropriate. Coverage may be suitable for businesses that require accessible and proportionate cyber insurance and incident-response support but do not require individually negotiated large-account cyber coverage.

For RPG business, eligible insureds must be members of the RPG, satisfy the agreed membership and underwriting criteria, and meet the applicable common or related liability-exposure requirements.

Types of customer for whom the product would be unsuitable

The product is not suitable for:

- individual or commercial customers that do not satisfy the applicable affinity scheme, membership or underwriting criteria;
- large or complex commercial entities requiring individually negotiated large-account cyber coverage, unless separately assessed and approved;
- customers requiring coverage that falls materially outside the approved policy wording;
- customers located in jurisdictions where the scheme, distribution structure or proposed coverage has not been approved such as the UK;
- individuals seeking cover for business, trade or professional activities under a personal cyber policy, unless the relevant activity is expressly covered;
- commercial entities attempting to insure personal or household exposures under a commercial cyber policy;
- customers with cybersecurity arrangements that do not satisfy applicable minimum eligibility requirements; or
- customers for whom the product would materially duplicate existing insurance without a clearly explained and appropriate interaction between the policies.

Any notable exclusions or circumstances where the product will not respond

Personal

(i) Limitations:
- Consultation with the Cyber Helpline prior to making a claim.
- Incidents to be reported no later than 30 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.

(ii) 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 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

Commercial

(i) Limitations:
- Any incurred loss during the waiting period as stated in the schedule will be uninsured.
- Incidents to be reported as soon a reasonably practicable.
- Insured to not make and payments, assume any obligations, incur expenses, enter onto any settlement without TMKS written consent.
- Accurate and complete information supplied to as requested.

(ii) Exclusions included but not limited to:
- Bodily injury
- Betterment
- Breach of contract, warranty, guarantee or promise and assumed liability.
- Loss of funds
- Terrorism
- Use of illegal or unlicensed programs or software
- War or uprising
- Insured misconduct

Other information which may be relevant to distributors

This product should be sold in line with FCA regulations and can only be sold by a regulated insurance distributor.

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.

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

This product can be sold via a Third-Party Online System, face to face, electronic communications or via telephone or a mix of these methods, if customers are provided with sufficient information to make an informed decision regarding the suitability of the product. This product may be sold both on an advised and non-advised basis.

Distribution Strategy:
- The distribution strategy for this product is to sell the product to a larger commercial entity, charity, affinity group, trade association, governing body, professional association or other approved affinity-based organisation who in turn can add value to their customers, members,

employees or participating organisations by offering an insurance solution that is designed specifically around their shared needs, interests and cyber risk exposures.

- Affinity programmes leverage collective purchasing power to negotiate competitive rates and comprehensive coverage options from insurance providers. This can result in cost savings, improved access to specialist cyber support services and more favourable insurance solutions than customers may be able to obtain when purchasing equivalent levels of cover on a standalone basis.

- The product may be distributed through approved affinity schemes, association programmes, group purchasing arrangements and, where approved, Risk Purchasing Group (RPG) structures, where collective purchasing gives eligible customers access to cyber cover and specialist services suited to their common needs and exposures. For RPG business, distribution is restricted to eligible RPG members with similar or related cyber liability exposures.

- Where members are automatically enrolled, customer communications and any customer portal must clearly explain the product, premium, coverage, significant exclusions, renewal arrangements, cancellation rights and opt-out process. The opt-out process should be straightforward and accessible and should not require evidence of alternative insurance.

Commission & Fees

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
- 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 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 Fair Value assessment completed	April 2025
Expected date of next assessment	May 2027