

Attorneys Insurance Mutual of the South NetGuard® Plus Cyber Liability Insurance Increased Limits Program

Law firms regularly maintain vast amounts of sensitive data, including personal and corporate information of clients, employees and even parties and witnesses in litigation. Should a data breach occur, law firms can be exposed to claims for liability, reputational harm and significant losses in complying with breach notification laws. Tokio Marine HCC - Cyber & Professional Lines Group ("TMHCC - CPLG") now offers a streamlined application process and simplified underwriting for Attorneys Insurance Mutual of the South ("AIM") policyholders who meet the NetGuard® Plus Cyber Liability Insurance program qualifications. Qualified Applicants can simply complete the Program Application, choose a limit, request to bind coverage and pay the applicable premium.

THIRD PARTY LIABILITY COVERAGE COMPONENTS

- **Multimedia Liability Coverage** – Coverage for defense costs and damages incurred in claims alleging liability resulting from the dissemination of online or offline multimedia material, including claims alleging copyright/trademark infringement, libel, slander, plagiarism or personal injury.
- **Security and Privacy Liability Coverage** – Coverage for defense costs and damages incurred in claims alleging liability resulting from a security breach or privacy breach, including failure to safeguard electronic or non-electronic confidential information or failure to prevent virus attacks, denial of service attacks or the transmission of malicious code from an insured computer system to the computer system of a third party.
- **Privacy Regulatory Defense and Penalties Coverage** - Coverage for defense costs and regulatory fines and penalties and/or regulatory compensatory awards incurred in privacy regulatory proceedings/investigations brought by federal, state, local or foreign governmental agencies.
- **PCI DSS Liability Coverage** – Coverage for defense costs and assessments, fines and penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.
- **Bodily Injury Liability Coverage** - Coverage for defense costs and damages incurred in claims alleging liability for bodily injury caused by a security breach or privacy breach.
- **Property Damage Liability Coverage** - Coverage for defense costs and damages incurred in claims alleging liability for failure to prevent or avoid property damage caused by a security breach or privacy breach.
- **TCPA Defense Coverage** – Defense-only coverage for claims alleging violation of the Telephone Consumer Protection Act, the Telemarketing and Consumer Fraud and Abuse Prevention Act, the CAN-Spam Act, or any similar federal, state, local or foreign law regulating the use of telephonic or electronic communications for solicitation purposes.

FIRST PARTY COVERAGE COMPONENTS

- **Breach Event Costs Coverage** – Coverage for reasonable and necessary mitigation costs and expenses incurred as a result of a privacy breach, security breach or adverse media report, such as legal expenses, public relations expenses, IT forensic expenses, breach notification costs (including voluntary notification costs), and the cost to set up call centers and provide credit monitoring and identity theft assistance.

- **Post Breach Remediation Costs Coverage** – Coverage for post-breach remediation costs incurred to mitigate the potential of a future security breach or privacy breach.
- **BrandGuard® Coverage** - Coverage for loss of net profit incurred as a direct result of an adverse media report or notification to affected individuals following a security breach or privacy breach. **A 2-week waiting period and 6-month period of indemnity apply to BrandGuard® coverage.**
- **System Failure Coverage** – Coverage for reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased, corrupted or stolen, and business income loss and interruption expenses incurred, due to an unplanned outage, interruption, failure, suspension, or degradation of service of an insured computer system, including any such incident caused by a hacking attack. **An 8-hour waiting period and 6-month period of restoration apply to the business interruption coverage component of System Failure.**
- **Dependent System Failure Coverage** – Coverage for reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased, corrupted or stolen, and business income loss and extra expenses incurred, due to an unplanned outage, interruption, failure, suspension, or degradation of service of an IT service provider computer system that is caused by specified cyber perils, including a denial of service attack, malicious code and acts of cyber terrorism. **A 12-hour waiting period and 4-month period of indemnity apply to the business interruption coverage component of Dependent System Failure.**
- **Cyber Extortion Coverage** – Coverage for extortion expenses incurred and extortion monies paid as a direct result of a credible cyber extortion threat.
- **Cyber Crime Coverage**
 - (1) **Financial Fraud** – Coverage for your loss of money or securities due to financial fraud, including wire transfer fraud;
 - (2) **Telecommunications and Utilities Fraud** – Coverage for (1) charges you incur for unauthorized calls resulting from the fraudulent use of an insured telephone system and (2) losses resulting from the fraudulent use of utilities, such as electricity, water, internet access and cloud computing; and
 - (3) **Phishing Fraud**
 - a) **Your Phishing Fraud Loss** – Coverage for your loss of money, securities or other property due to phishing schemes that trick an Insured to transfer, pay or deliver money, securities or other property to an unintended third party, plus expenses incurred to notify your clients or customers of such phishing fraud.
 - b) **Client Phishing Fraud Loss** – Coverage for your loss of money, securities or other property which your client, customer or vendor intended to pay to you, but which was paid to an unintended third party due to a phishing scheme that tricked your client, customer or vendor by impersonating an Insured, plus the cost of reimbursing your customers, clients or vendors for their own losses that result from such phishing schemes.
- **Bricking Loss Coverage** – Coverage for the costs incurred to replace computer hardware or electronic equipment that has been rendered nonfunctional due to a hacking attack, up to 125% of replacement value.
- **Property Damage Loss Coverage** – Coverage for damage to your property resulting from a hacking attack.
- **Reward Expenses Coverage** – Coverage for reasonable amounts paid to an informant for information not otherwise available, which leads to the arrest and conviction of a person or group responsible for a privacy breach, security breach, system failure, cyber extortion threat, financial fraud, telecommunications fraud, or phishing attack.
- **Court Attendance Costs Coverage** – Coverage for reasonable costs incurred to attend court, arbitration, mediation, or other legal proceedings or hearings as a witness in a claim covered under the policy.