Enterprise Cyber Liability Program

Data Security is a paramount concern to risk managers and businesses around the world. Whether a business maintains confidential employee data, customer information such as credit card data, or confidential client information, really any private, non-public information of any kind in an organization's care, custody or control, maintaining the security and privacy of this information is critical. A breach of data security could be ruinous in terms of costs to comply with state notification requirements, potential liability claims, and damage to a company's reputation. The Enterprise Cyber Liability Program protects businesses for these associated costs of an actual or suspected violation of a privacy regulation due to a security breach that results in the unauthorized release of protected personal information.

The Enterprise Cyber Liability Program also provides value-added risk management, crisis management and public relations services. In the event of a data breach, legal assistance is just a phone call away.

The Enterprise Cyber Liability Program is facilitated through the North American Data Security RPG (named insured on the master policy), a risk purchasing group which is registered in all 50 states and the District of Columbia. The master policy is underwritten by AXIS Insurance Company, an A+ rated insurance carrier by AM Best.

POLICY DETAILS

• Limit of Liability:

• $250,000 (annual aggregate limit of liability per enrollee)
• Policy form (admitted) is claims made with full prior acts
• First dollar coverage (no deductible)
• Coverage territory is worldwide
• Claim reporting requirement - within 60 days upon becoming aware of a suspected or actual breach
• Ineligible businesses:
  - Businesses that process greater than 6mm payment card transactions annually with a card brand (i.e. VISA) or; a business that has experienced a breach of payment card data, or; deemed Level 1 by a card brand

COVERAGE DETAILS

• Civil proceeding or investigation including requests for information for an actual or alleged violation of any privacy regulation (PII data) brought on behalf of any federal, state, or foreign governmental agency including;

- Defense & settlement or judgment
- Regulatory fines & penalties (including PCI)
- Mandatory forensic examination

- PCI re-certification to re-certify compliance with PCI Security Standards
- Wrongful conduct of rogue employee
- Automatic subsidiary coverage including newly created and acquired entities

- Ransomware - $10,000 sub-limit applies
- Telecommunications Theft - $10,000 sub-limit applies
- Social Engineering Fraud - $10,000 sub-limit apliies
- E-Theft - $100,000 sub-limit applies

• Crisis management and fraud prevention expense:

Notification	Credit monitoring
Call Center	Public relations
Forensics	Associated legal expenses

PROGRAM ADMINISTRATION

- Claim service offered 24 X 7
- No application required
- Website includes program FAQ, certificate of insurance, policy terms and conditions, claim reporting and contact information

CLAIM EXAMPLES

The claim examples below illustrate the types of exposures companies face:

A dental practice found a ransomware demand for $4,900 on a computer which contained protected health information ("PHI") on 3,780 patients. In addition to paying the ransom, the dental practice incurred the following expenses: forensics, legal services, breach notification expenses, identity restoration and credit monitoring and public relations expenses which totaled $49,428.79

A residential contractor became a victim of a social engineering attack and wired $35,000 to criminals after receiving fraudulent instructions from a criminal posing as a vendor.

A restaurant in Washington was notified of a breach by MasterCard due to a high level of fraud. They were required to immediately undergo a forensic examination which totaled $11,646.90. Six months later, the restaurant was fined $26,242 for Fraud Recovery along with a Case Management Fee of $8,000. Two months later, Visa assessed a non-compliance fine of $5,000. The restaurant had a total cost of $50,888.90 due to this breach

A medical practice closed it doors after hackers deleted all of its patient records when doctors refused to pay a ransom. The two doctors who were partners decided to retire early rather than try to rebuild the practice. The doctors refused to pay hackers a $6,500 ransom in exchange for a code to access the practice's medical files. The hackers deleted all the records, including files, appointment schedules, payment, and patient information.

For additional information, please contact 1-888-747-8220 Ext. 811

This is a brief coverage summary, not a legal contract. The actual policy should be reviewed for specific terms, conditions, limitations, and exclusions that will govern in the event of loss. Extended sixty day reporting period applies.

May 2019