Claims examples for all insuring modules

ASCENT™ UNDERWRITING

This list is for illustrative purposes only and it does not in any way constitute a definitive guide as to coverage. All claims notified are subject to their own unique facts and coverage is assessed on a case by case basis.

1 NETWORK SECURITY CLAIM

Ransomware was installed on the Insured's computer network, which resulted in their files being encrypted. A ransom demand of 2.5 Bitcoins (approximately $1,100) was then made. The Insured paid the ransom and received a key to unlock the encrypted files. However, the key only unlocked some of the files, while others remained encrypted.

An IT solutions firm was then retained to assist in restoring the encrypted data. Breach counsel was also retained to assess the potential to notify any individuals who may have had personally identifiable information compromised. Forensics decrypted all the files and has wiped the infected servers clean and removed all ransomware, restoring the Insured's data.

Forensics work, and breach counsel fees were covered under the policy. The Ransomware was not covered in this instance because the insured failed to give insurers the opportunity to first test the encryption key. Ordinarily ransom will be covered.

2 SOCIAL ENGINEERING

The insureds accountant received an email from the insured, requesting a wire transfer of $16,941 to a third party to facilitate a real estate transaction, the accountant complied with the request. The accountant received a further request for a wire transfer in the sum of $37,901. Due to the unusual nature of the request, the Insured's financial consultant was contacted, and it was shortly discovered that both requests were fraudulent. Insurers indemnified the losses after policy deductible.

3 TECHNOLOGY

The insured provides IT services including server management. It used a technology data synchronise system to move data between windows file servers. The data technology company was troubleshooting an issue with data synchronisation which resulted in thousands of files being deleted. Kroll Ontrack was retained to back up the file servers. This was successfully completed but it took 2 months to complete. The insured was covered for the damages liability to its customer and claims expenses under the insuring module Technology Services.

4 BILLINGS ERRORS & OMISSIONS

The insured received a letter from the Centres for Medicare & Medicaid Services ("CMS") advising that Medicare overpaid the insured in error in the amount of $230,000. The amount of the overpayment and entitlement to a refund is currently the subject of litigation. Defence costs are being met by Insurers.

5 ELECTRONIC THEFT, COMPUTER FRAUD

The Insured's client's email accounts were hacked. The Insured received an email, purportedly from the client, asking for a payroll payment of $12,250 which it duly made to the fraudster's account. Insurers indemnified the loss under insuring module 9 Electronic Theft, Computer Fraud.

6 EVENT SUPPORT EXPENSES

The Insured's temporary employee mis-mailed/addressed eighty-two 1099 Forms containing PII, such as Social Security Numbers and entity Tax Identification Numbers. The event was discovered when one of the Insured's clients contacted the Insured's CFO to advise that he (the client) had incorrectly received a Form 1099 that belonged to another entity. The Insured, on insurers recommendation, retained the services of Breach Counsel to deal with Federal authorities and reporting obligations.

The expenses incurred in this matter fell within the Insured's Deductible.

Claims examples for all insuring modules

ASCENT™ UNDERWRITING

7 MISCELLANEOUS PROFESSIONAL SERVICES

The insured received a civil complaint alleging that it sent 889 illegal unsolicited commercial " email advertisements which went through the Plaintiff's email server. The Plaintiff alleged that the Insured is responsible for transmitting all the emails and sought damages.

Insurers provided defence costs pursuant to Insuring Module 4 - Miscellaneous Professional Services.

8 MULTIMEDIA AND INTELLECTUAL PROPERTY LIABILITY

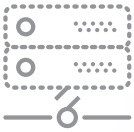
The insured hosted a website retail manufacturing business which promotes the sale of various goods subject to trademark and/or copyright protection. The Insured was sued by a third party for breach of Intellectual property rights. The Plaintiff sought unspecified damages, delivery up of the goods and an account of profits. Cover for the claim and defence costs was provided under insuring Module 2.

9 SECURITY AND PRIVACY LIABILITY

The Insured, is a multi-clinical network with a wide array of primary care, specialty and referral services. The Insured provides services to more than 35,000 insured and uninsured patients annually.

The Insured was notified by a member of public that he found PHI in a folder in his home. The documents contained the name, address, social security numbers and date of births of 60 individuals who were applying to receive medical services. The Insured later discovered that one of its Executive Assistants had taken the documents to her relative's home to catch up on her work. The insured was covered under our security and privacy liability module for all notification and credit monitoring expenses.

10 NETWORK INTERRUPTION AND RECOVERY



The Insured's network suffered a ransomware attack. This network event affected several different directories and applications, and insurers conclude that this was a security event which triggered the Policy's coverage. This event was covered under Insuring Module 5 of the Ascent Cyberpro Policy.

It took the IT Forensic experts a full week to clean and reset insureds network. The servers and applications have now been fully restored.

11 NETWORK EXTORTION

The insured, discovered that one of its computer servers had been infected by a variant of the CrySIS ransomware virus known as the Dharma Variant. The hacker demanded a payment of 6 bitcoins -$7,607.94 (valuation at the time of the event) to provide a decryption key. The insured contacted its third-party IT company but they could not restore the data through backups. Insurer's IT Forensic experts took the view that the ransom should be paid. The decryption key decrypted most files and the forensic experts were able to restore and decrypt the remaining files. Coverage was given under Insuring Module 5 Network Extortion.

12 PRIVACY REGULATORY DEFENSE AND PENALTIES

The insured was served with a lawsuit alleging violations of the Americans with Disabilities Act ("ADA"), violations of the Electronic Communications Privacy Act ("ECPA") and trespass. The Plaintiff was visually impaired and it was claimed that the insured's website did not have the usual applications to accommodate visually impaired consumers since the privacy policy could not be read and the violation of ECPA was because there was an actionable trespass due to cookie storage. This matter is covered under module 7 privacy regulatory defense and penalties.