Could This Happen to You?

Cyber Liability Scenarios

CMG Member Claims Examples

Diocese A

01CMG22299

- An employee of the Insured opened an e-mail that triggered a cryptolocker virus.
- The associated ransom was $450, and the virus migrated to several computers.
- Rather than pay the ransom, the Insured wanted to get a forensics company involved.
- NAS helped them find a vendor, who unencrypted their records. While the vendor was performing forensic services, the Insured was able to recreate some of their data from paper records so it could be accessed immediately.
- To date, we have paid $2,000 to the vendor and await further invoices. We also await the Insured's documentation of the extra employee time spent working on the data. The Diocese currently has $15,000 in reserves.

Date of Loss 03/22/2016

Archdiocese B

01CMG21282

- The Insured's third party vendor for payroll services, Ultipro, experienced a hacking incident. The hackers spent several hours viewing employees' private information (W-2 forms); the initial estimated number of potentially affected employees was 1,000-4,000.
- After completing an investigation, counsel concluded that only 78 employees were actually affected. Notification letters and free credit monitoring were sent.
- A couple months later, several of the Insured's employees reported incidents of identity theft – bogus tax returns were filed with the IRS using their personal information.
- Unfortunately, the affected employees had not been included in the initial group of 78, which led to the Insured being concerned about whether their systems – rather than their vendor's systems – had been breached.
- We retained a forensic vendor, and also provided proactive protection and remediation services for the affected parties. Reserves are now $105,000.

Date of Loss 10/27/2015

Diocese C

01CMG22192

- The Insured was hit with a ransom virus and a demand for $250.
- They did not want to pay the ransom, and instead retained a local IT group who successfully unencrypted the data. A $10,000 reserve was created.
- Fortunately, the IT group worked quickly, and costs were less than $1,000. We anticipate closing this file soon.

Date of Loss 03/11/2016

Diocese D
01CMG19205

- A burglary occurred at a local High School, and several laptops were stolen, including that of the school's principal, which contained personal information on parents and donors. In addition, a safe containing checks and credit cards was stolen.
- We appointed counsel to assist the Insured in evaluating the necessity of notification to potentially affected parties. Approximately 2,100 persons were notified.
- The claim is closed; paid $3,774 in notification costs expenses.

Date of Loss 11/20/2014

NAS Carrier Large Claims Examples

The following scenarios are examples of the types of claims and associated costs commonly seen and do not represent a comprehensive explanation of any one particular claim. While the subject coverage is designed to address certain risks and associated costs, coverage may not be available in all circumstances. Each reported claim will be evaluated on a case-by-case basis. The actual policy or endorsement language should be referenced to determine coverage applicability and availability.

Example 1

Privacy Regulatory Defense and Penalties

- In 2015, a large cable communications company suffered a data breach due to a form of social engineering called “pretexting” in which an individual tricks another party into divulging confidential information. In this case, the hacker pretended to be an employee in the company’s IT department and convinced two individuals - a Customer Service Representative and contractor - to enter their company IDs and passwords into a fake, or “phishing” website.

- The hacker used the employee security credentials to access the personally identifiable information (“PII”) and customer proprietary network information (“CPNI”) of customers. The breach exposed customers’ names, home addresses, email addresses, phone numbers, partial social security numbers, driver’s license numbers, and telephone numbers.

Example 1 (cont'd)

Privacy Regulatory Defense and Penalties

- The Federal Communications Commission (FCC) investigated and found that a lack of technical safeguards, such as multi-factor authentication, contributed to the individual's ability to access the information. The breach resulted in the hacker posting the PII of at least eight individuals on social media sites, changing the passwords of at least 28 customers and sharing customer PII with another hacker.

- The FCC also found that the company failed to report the data breach through the FCC's data breach portal, as required by law.

- At the conclusion of its investigation, the FCC ordered the company to pay $595,000 in civil penalties, notify all customers of the breach, and provide free credit monitoring to affected individuals.

Source: FCC.gov, Nov 5, 2015 - News Release, Press release for Cox Communications consent decree, (accessed April 11, 2016)
https://apps.fcc.gov/edocs_public/attachmatch/DOC-336222A1.pdf

Example 2

Privacy Regulatory Defense and Penalties

- A large hospital notified the Office for Civil Rights (OCR) that a laptop was stolen from an unlocked treatment room during the overnight hours in 2011. The laptop was on a stand that accompanied a portable CT scanner and contained the protected health information (PHI) of 599 individuals.

- Evidence obtained through OCR's subsequent investigation indicated widespread non-compliance with the HIPAA rules, including:
  - Failure to conduct a thorough risk analysis of all of its ePHI;
  - Failure to physically safeguard a workstation that accessed ePHI;
  - Failure to implement and maintain policies and procedures regarding the safeguarding of ePHI maintained on workstations utilized in connection with diagnostic/laboratory equipment;
  - Lack of a unique user name for identifying and tracking user identity with respect to the workstation at issue in this incident;
  - Failure to implement procedures that recorded and examined activity in the workstation at issue in this incident; and
  - Impermissible disclosure of 599 individuals' PHI

Example 2 (cont'd)

Privacy Regulatory Defense and Penalties

- In 2015, the hospital agreed to pay $850,000 to settle potential HIPAA violations.

Source: HHS.gov – release: "HIPAA Settlement Reinforces Lessons for Users of Medical Devices" (November 25, 2015), http://www.hhs.gov/about/news/2015/11/25/hipaa-settlement-reinforces-lessons-users-medical-devices.html (accessed April 28, 2016).

Example 3

Privacy Breach Response Costs, Customer Notification Expenses, and Breach Support and Credit Monitoring Expenses

- A regional life insurance company moved to new offices. During the office relocation, several laptops, desktops and printers were stolen. While the desktops were secured and did not contain personal data, one of the laptops did contain over 36,000 records (PII and PHI) related to the insurance policyholders.

- Because of the size and nature of the breach, the Office for Civil Rights (OCR) was also notified. The OCR investigation was closed without an assessment of fines and penalties because of Insured had demonstrated they took multiple voluntary actions to ensure future compliance with privacy regulations.

- Forensic investigations, legal fees, and notification expenses were over $200,000.