

Security & Privacy

Claims Scenarios

Financial Institutions

Hacking:

- **Incident:** Financial institution's network suffered a security breach. Hackers broke into the insured's system and inflated the balances of 100 issued payroll and prepaid debit cards to \$250,000 per card. Track data and personal identification numbers were used to make counterfeit cards, which were used repeatedly in over 300 ATM locations, located in 20 countries over a seven day period. Approximately \$14,000,000 in such transactions were ultimately processed.
- **Executive Liability Payment:** Reimbursed the insured for the \$14,000,000 loss and paid \$2,000,000 for crisis management, notification costs, and public relations services.

Rogue Employee:

- **Incident:** A rouge employee used a personal USB drive on the company computer system to steal and sell the identities of over 4,000,000 customers and applicants.
- **Executive Liability Payment:** Proposed settlement exceeds \$15,000,000 and includes credit monitoring services, identity theft insurance, and attorney fees.

Lost/Stolen Equipment:

- **Incident:** E-mail server and external hard drive containing personally identifiable customer information was stolen while in the custody of an outside vendor. The information was in the possession of the vendor to facilitate an investigatory request. An employee of the outside vendor has been implicated.
- **Executive Liability Payment:** While no lawsuit was filed, Chartis paid out over \$3,000,000 in crisis expenses for legal advice, public relations, forensics, and notification costs.

Healthcare

Rogue Employee:

- **Incident:** Rogue employee at a large medical provider stole and sold over 40,000 patient records containing personally identifiable information.
- **Executive Liability Payment:** Reimbursed the insured over \$700,000 for notification and credit monitoring costs.

Lost/Stolen Equipment:

- **Incident:** Insured lost tapes containing medical insurance information and Social Security Numbers.
- **Executive Liability Payment:** Reimbursed the insured \$400,000 for call center services and credit monitoring costs. Further expenses pending.

Education

Error/Negligence:

- **Incident:** Insured accidentally published confidential information regarding 117,000 students on their website. The insured hired forensic experts to determine the precise amount of information, and number of students who were affected. Additionally, the insured sent notification letters to all impacted students and a call center was created to address concerns of the affected students.
- **Executive Liability Payment:** Reimbursed the insured \$100,000 for call center services, forensic investigation, credit monitoring, and public relations services.

Error/Negligence (Regulatory Action):

- **Incident:** Insured accidentally made confidential information regarding approximately 42,000 students available on its website. A parent of one of the affected students filed a potential class action lawsuit alleging that the insured violated her child's privacy rights and that the insured was negligent in failing to properly protect the student's privacy. Additionally, the Federal Trade Commission launched an investigation to determine if the insured complied with the FTC Act which prohibits misrepresentations about privacy practices.
- **Executive Liability Payment:** Paid out \$250,000 in legal defense costs pursuant to the regulatory action sublimit of liability.

Lost/Stolen Equipment:

- **Incident:** Employee of a medical college lost a USB drive while traveling from a teaching hospital to the college office. The drive contained personally identifiable information of 2,000 hospital resident applicants. The college alerted the hospital, notified the affected individuals, and contracted credit and identity monitoring services.
- **Executive Liability Payment:** Reimbursed the insured over \$57,000 for notification and credit monitoring costs.

Error/Negligence:

- **Incident:** Employee of a college accidentally mass emailed a file containing the personal information of approximately 23,000 students. The insured sent a notification letter to affected students and set up a call center.
- **Executive Liability Payment:** Reimbursed the insured over \$38,000 for call center and notification costs.

Retailers

Rogue Employee:

- **Incident:** Insured was sued when an employee misappropriated confidential information from a competitor.
- **Executive Liability Payment:** Settled and paid approximately \$200,000.

Hacking:

- **Incident:** Hackers gained access to the computer systems of 26 hotel locations and were able to access the names and credit card numbers of approximately 480,000 individuals.
- **Executive Liability Payment:** Reimbursed the insured over \$980,000 for crisis management related expenses.

Rogue Employee:

- **Incident:** Rogue employee at a large consumer reporting agency illegally stole and sold personal information of over 3,000,000 customers.
- **Executive Liability Payment:** Paid over \$5,100,000 in damages, over \$1,000,000 in legal defense costs, and reimbursed the insured \$1,000,000 for notification and credit monitoring costs.

Payment Processors

Hacking:

- **Incident:** Payment card processor's system was hacked compromising credit card data.
- **Executive Liability Payment:** Paid over \$20,000,000 in legal defenses and crisis management related expenses.

Hacking:

- **Incident:** The insured is a credit card processor for small to mid-sized businesses. Hackers broke into the insured's database and accessed consumers' personal data. This resulted in a class action lawsuit, which was filed against the insured alleging that the insured improperly stored unencrypted customer data, and failed to maintain proper firewall protection.
- **Executive Liability Payment:** Settled for \$1,250,000 and paid over \$160,000 in defense costs.

Technology/Telecom

3rd Party/Outsourcer:

- **Incident:** A printer wrongfully provided credit card information to a third party resulting in unauthorized transactions for its customers.
- **Executive Liability Payment:** Paid over \$440,000 in legal defenses.

Hacking:

- **Incident:** ATM network security breach resulting in a total loss of \$2,200,000 to bank customers. Unidentified individuals gained unauthorized access to the insured's operating systems enabling them to steal debit card account information. The resulting lawsuit alleged negligence for the fraudulent use of over 400 debit cards. Each of the debit cards had previously been legitimately used at ATM locations in New York.
- **Executive Liability Payment:** Paid over \$2,430,000 in indemnity and defense costs.

To learn more about Security & Privacy Insurance, please visit www.chartisinsurance.com, e-mail executiveliability@chartisinsurance.com, or contact your insurance broker.

175 Water Street
New York, NY 10038
www.chartisinsurance.com



Chartis is a world leading property-casualty and general insurance organization serving more than 45 million clients in over 160 countries and jurisdictions. With a 90-year history, one of the industry's most extensive ranges of products and services, deep claims expertise and excellent financial strength, Chartis enables its commercial and personal insurance clients alike to manage virtually any risk with confidence.

Chartis is the marketing name for the worldwide property-casualty and general insurance operations of Chartis Inc. For additional information, please visit our website at www.chartisinsurance.com. All products are written by insurance company subsidiaries or affiliates of Chartis Inc. Coverage may not be available in all jurisdictions and is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain coverage may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds and insureds are therefore not protected by such funds.