Wayne E. Bernstien - Director, Professional Lines
40 W. Cochran Street, Suite 203/205
Simi Valley, CA 93065
wayneb@monarchexcess.com; 805-577-6800 Ext. 223

Cyber Liability and Data Security +

Claim Examples

COVERAGE PART A

- **Data Breach Liability:** Alice owns a restaurant whose point of sale machines had been illegally skimmed with a small, hidden electronic device for eight months, affecting nearly 1,000 cards. Over those eight months, some cardholders became identity theft victims, and paid for their own credit monitoring; others had debit cards skimmed and were not able to recover stolen funds from their bank accounts because too much time had expired without them noticing the fraudulent activity. Victims banded together and sued the store for costs incurred, including paying for credit monitoring, recovering lost funds and expenses incurred in clearing their identity.
- **Security Breach Liability:** Diane's real estate agency is sued by an e-commerce organization for its participation in a denial of service attack against the e-commerce firm. Diane's agency had antivirus and firewall protection on its computers; however, the firm had not made updates to them in the past couple years. It turns out their computers became infected with malware, which, when activated, participated in an attack against the e-commerce firm's servers, overloading them with requests and shutting down their system for a day. The e-commerce firm sued the agency, among others for lost revenue and costs to repair their server as a result of the neglect of standards of care by those unknowingly participating in the attack. Diane's agency paid over $50,000 in defense and settled for $30,000 in loss.
- **Defense of Regulatory Proceedings:** Joe owns an appliance sales organization. Joe makes the decision to store client names, addresses, phone numbers and spending habits to help cross-sell their other products. The organization does not have proper security in place to protect the information. A hacker gains access to the personal information and sells it on the Internet. The state where the merchant is located accuses them of privacy law violations and sets up hearings to decide if fines will be asessed. Joe expends $10,000 to defend the company and is ultimately fined $30,000.
- **Payment Card Industry (PCI) Fines & Penalties:** A small family restaurant in Utah was informed by their payment card-processing bank of a potential data breach of their point-of-sale system. A forensics investigation found they unintentionally stored credit card numbers. However, the payment card processor demanded indemnification for fines assessed by the credit card companies who alleged a data breach. The payment card processor withdrew $10,000 from the restaurant's bank account and sued them for the balance of $80,000.