

Dentists' Claim Scenarios

CNA NetProtect EssentialSM provides Privacy, Identity Theft and Network Security Liability coverage for any company that relies on electronically stored information. Simple, daily tasks, such as storing sensitive information on your network or connecting to the Internet, make your network a resource that can be exploited. Below are claim scenarios that depict how CNA NetProtect EssentialSM may help protect your dental practice.

A dentist's practice sustains a network security breach. The system attack compromises patient records and financial information and health benefits account data is taken. Data is resold to individuals who use benefits information to fraudulently obtain dental services. Legitimate patients sue, seeking compensation for emotional distress in addition to other consequential damages. The legitimate patients' health insurance carriers sue the dentist's practice to recover reimbursements made for fraudulently obtained dental services.

A hacker penetrates a dentist's network security and steals credit card information from a database containing stored transaction data. The hacker uses the harvested information to make purchases and to fraudulently obtain loans in each cardholder's name. Cardholders sue the dentist to recover their cost to repair credit and discharge fraudulent loans. They also seek damages for emotional distress. The banks who issued the cards compromised in the attack sue the retailer to recover card reissuance and cardholder notification costs.

An offshore identity theft ring installs a keystroke logger (spyware) on a dentist's network. The spyware captures confidential information, including passwords, login data and account details exchanged between the dentist and dental insurance providers or financial payment vendors handling credit card transactions. The spyware relays this private information to the offshore theft ring. Harvested data is subsequently used to fraudulently obtain loans in the names of the dentist's patients. The patients discover the compromise when reconciling account statements and upon receipt of late payment notices on loans they never took out. Patients sue the dentist for consequential damages resulting from failure to protect their private financial information.

A dental practice maintains a Web site to promote its services. An attacker defeats the site's security and plants a "bot" on the site. The "bot" is designed to generate Web traffic in coordination with similar "bots" installed on other innocent sites. The Web traffic generated by all sites combined is used in a Denial of Service (DOS) attack, which floods a security dealer's network with enough traffic to disrupt securities transactions. The securities dealer sues all the sites involved in the DOS attack. The suit seeks compensatory damages for lost income resulting from the disrupted securities transactions.

For more information, please contact:

Professional Services Plans (PSP)
A Division of Brown & Brown, Inc.
3101 W. Dr. Martin Luther King Blvd, Suite 400
Tampa, FL 33607
800-467-8734

