Media Notice

Delta Dental of California and affiliates[1] ("Company") experienced a data security incident involving the MOVEit Transfer ("MOVEit") software, an application used by the company and many organizations worldwide. The Company is notifying impacted individuals of a data security incident that may have involved a limited amount of those individuals' protected health information or personal information, including information shared in connection with dental procedures and names with some combination of the following: addresses, Social Security numbers, driver's license numbers or other state identification numbers, passport numbers, financial account information, tax identification numbers, individual health insurance policy numbers, and/or health information.

Progress Software Corporation announced a previously unknown vulnerability within their widely used MOVEit software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more.

On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, the Company launched a thorough investigation and took steps to contain and remediate the incident. The Company stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity.

On July 6, 2023, the incident investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023, and May 30, 2023. At that time, the Company promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated.

This extensive investigation and analysis of the data recently concluded and was a critical component in enabling the Company to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, the Company has worked

[1] The Delta Dental of California enterprise includes its affiliates Delta Dental Insurance Company, Delta Dental of the District of Columbia, Delta Dental of Delaware, Inc., Delta Dental of Pennsylvania, Delta Dental of New York, Inc., Delta Dental of West Virginia, and their affiliated companies, as well as the national DeltaCare USA* network, and covers enrollees in all 50 states, plus Washington, D.C. and Puerto Rico.

*DeltaCare USA is underwritten in these states by these entities: AL — Alpha Dental of Alabama, Inc.; AZ — Alpha Dental of Arizona, Inc.; CA — Delta Dental of California; AR, CO, IA, MA, ME, MI, MN, NC, ND, NE, NH, OK, OR, RI, SC, SD, VT, WA, WI, WY — Dentegra Insurance Company; AK, CT, DC, DE, FL, GA, KS, LA, MS, MT, TN, WV — Delta Dental Insurance Company; HI, ID, IL, IN, KY, MD, MO, NJ, OH, TX — Alpha Dental Programs, Inc.; NV — Alpha Dental of Nevada, Inc.; UT — Alpha Dental of Utah, Inc.; NM — Alpha Dental of New Mexico, Inc.; NY — Delta Dental of New York, Inc.; PA — Delta Dental of Pennsylvania; VA — Delta Dental of Virginia. Delta Dental Insurance Company acts as the DeltaCare USA administrator in all these states.

diligently to identify any impacted individuals to provide notification. In addition to its own investigation, the Company has also notified law enforcement of the incident and has been cooperating with them since. The investigation into the affected information was completed on November 27, 2023.

Data security is a priority for the Company. The Company applies security patches for known vulnerabilities provided by third-party software vendors, regularly updates its capabilities to monitor potential security threats and consistently manages access to its systems and data.

Letters with more information about the incident, as well as instructions for enrolling in credit monitoring and identity protection services at no cost, are being mailed to individuals for whom addresses are available. The Company encourages individuals to remain vigilant by reviewing their bank accounts, credit reports, other financial statements and explanation of benefits closely and immediately report any suspicious activity to the company that maintains the account for the individual.

Impacted individuals can call 800-693-2571 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time with questions. The Company takes seriously the need to protect the privacy and security of all information in its care and regrets any inconvenience or concern that this matter may cause.