Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
February 6, 2024

RE: Data Security Event

Arch Capital Services LLC ("Arch Services") is submitting this notice to provide your office with information regarding a vendor cybersecurity event that resulted in unauthorized access to employee personal information ("PI"). Arch Capital Group Ltd. (together with its subsidiaries, "Arch") is based in Bermuda and provides insurance and reinsurance products through its wholly-owned subsidiaries. Arch Services is a wholly owned subsidiary of Arch Capital Group Ltd., and provides corporate, legal, and other support services to Arch. This incident did not directly affect Arch or Arch Services operations or any of their systems, but did affect participants in Arch Services' employer sponsored dental plan through its plan administrator Delta Dental.

On January 24, 2024, Delta Dental informed Arch Services that it had experienced a cybersecurity incident which impacted the personal information of some US employees of Arch Services' affiliates who participate in the plan and their beneficiaries (collectively "Plan Participants"). Delta Dental had provided an initial notice that they were experiencing a cybersecurity incident in June of 2023, but were unable to confirm that this incident affected Arch Services data or Plan Participants until January 24, 2024. Delta Dental serves as the plan administrator for Arch Services' employer sponsored optional dental insurance plan as part of Arch's employee benefits package for US employees. According to Delta Dental, unauthorized actors exploited a vulnerability in the MOVEit Transfer software application to acquire personal information between May 27 and May 30, 2023. Delta Dental reports it learned of the incident on June 1 and promptly engaged third-party forensic experts to conduct an investigation into the affected information. On January 24, 2024 Delta Dental informed Arch Services of the incident and that the personal information of 26 Plan Participants in your state were affected. Affected personal information includes

.

No Arch system was impacted.

Delta Dental reports that it has taken steps to remediate the incident and to help prevent similar incidents in the future, including by enhancing its existing cybersecurity controls. Delta has also contacted law enforcement and regulators concerning the incident. We understand Delta Dental is providing all affected individuals, including Plan Participants, with of complimentary identity theft protection and credit monitoring through Kroll. We understand from Delta Dental that these notices have already been made or are in the process of being made.

Arch regularly monitors the cybersecurity risk of their vendors and uses various means to mitigate that risk. The contract between Arch Services and Delta Dental contains provisions requiring Delta Dental to maintain safeguards to protect the confidentiality and security of employee personal information. Arch Services is also monitoring Delta Dental's cybersecurity risk through its SOC 2 certifications, and will continue to do so going forward. Arch Services' relationship with Delta Dental is also governed by a HIPAA compliant business associate agreement.

At this time, we consider the incident to be resolved. We will update your office as to any material developments.

Should you have any questions please do not hesitate to contact our outside counsel:

560 Mission Street
Suite 1300
San Francisco, CA 94105

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Notice of Data Security Incident / Notice of Data Breach - CA residents only)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Delta Dental of California and affiliates ("Company")[1] experienced a data security incident involving the MOVEit Transfer ("MOVEit") software, an application used by our company and many organizations worldwide. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter provides information about what happened, how to help protect your information and resources offered to assist you.

What Happened?

Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer 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, we launched a thorough investigation and took steps to contain and remediate the incident. We 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, our 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, we 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 us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.

[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.

What Information Was Involved?

Your affected information included, **<<b2b_text_2(data elements)>>.**

What We Are Doing:

In addition to the steps already described, we are offering you **of free** identity monitoring services through Kroll. To take advantage of these free services, please follow the instructions below.

Data security is a priority for our Company. We apply security patches for known vulnerabilities provided by third-party software vendors, regularly update our capabilities to monitor potential security threats and consistently manage access to our systems and data.

What You Can Do:

We encourage you to remain vigilant by reviewing your account statements and credit reports closely and immediately reporting any suspicious activity to the company that maintains the account for you. At the end of this letter, we have provided you with additional information regarding steps you can take to help protect yourself and your personal information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. **We encourage you to review that additional information.**

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for twenty-four months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

For More Information:

If you have questions, please call TFN, 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, excluding major U.S. holidays. Please have your membership number ready. Helping protect your information is important to us. We sincerely apologize for any inconvenience this incident may cause you.

Sincerely,

Delta Dental of California and affiliates

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to **https://enroll.krollmonitoring.com** and follow instructions for enrollment using your Membership Number provided in the letter.

2. Activate the credit monitoring provided as part of your Kroll identity monitoring membership. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, Kroll will be able to assist you.

3. Telephone. Contact Kroll at TFN to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. XX Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.