

## Letter to the HCPS Community Regarding the Delta Dental/MOVEit Data Breach

HCPS recently learned that in May of 2023, our former dental insurance carrier, Delta Dental, experienced a data breach in their MOVEit file-transfer software program.

We have learned Delta was one of the many organizations impacted by their data security incident resulting from a previously unknown vulnerability in the MOVEit file transfer software, which is owned by Progress Software. The breach has impacted many organizations, insurance providers, and financial institutions, with an estimated 7 million individuals being impacted by this data breach. Unfortunately, HCPS has not been provided information from Delta regarding the number of HCPS employees and retirees impacted by the data breach or more information beyond the letters impacted individuals may have received.

From our understanding, this breach compromised personal identifying information, including name, address, social security number, date of birth, and healthcare information.

Delta Dental has mailed letters to those who were impacted by the breach, detailing the information compromised in their account, instructions, and a membership number for enrolling in 24 months of free credit monitoring and identifying theft protection through Kroll. **If you did not receive a letter from Delta Dental, you may not be impacted by this data breach.** HCPS has not been provided information from Delta regarding the number of HCPS employees and retirees impacted by the data breach or more information beyond the letters impacted individuals may have received.

If you have questions about the data breach or need additional information on the identity theft protection program, **the Kroll customer service team is available Monday through Friday at 1-800-693-2571**, from 8:00 a.m. to 5:30 p.m. (Central Time), except for major U.S. holiday closures.

Please note that the HCPS Benefits Office does not have additional details regarding this incident.

### What you should do to protect your personal and financial information:

- **If you receive a letter from Delta Dental, take advantage of the free credit monitoring and identity theft protection:** Information and a unique membership number for registering in the program will be contained in the letter from Delta Dental. You must activate this protection within 90 days of receiving the letter.
- **Monitor and set up alerts for bank accounts:** Monitor your bank account(s) for suspicious transactions and report any to your bank. Ask the bank for online monitoring and alerts on your account. This will give you an early warning of any fraudulent transactions.
- **Watch out for suspicious emails, phone calls, and text messages:** It is possible that the person(s) behind this attack may send threatening communications in an attempt to scare people into giving them money. If you receive such communication, forward it to your local authorities or delete it. Do not respond or engage to these messages.
- **Place a fraud alert on your credit file:** We recommend you place a fraud alert on your credit file by contacting one of the three nationwide credit bureaus listed below. If a fraud alert is placed on a consumer's credit file, specific identity verification steps must be taken before extending new credit.
- **Important reminders about protecting yourself:** These incidents are reminders of the importance of doing everything possible to protect your online information.