dexcom

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

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

Notice of Data Breach

Dexcom, Inc. ("Dexcom" or "we") recognizes the importance of protecting your personal information and is committed to handling it responsibly. We write to inform you of an incident that involved some of that information. Please read this notice carefully, as it provides information about the incident, the personal information that was involved, the steps we have taken to address the incident, and the steps you may consider taking to help protect your information. We have included our contact details below should you need any further information.

What Happened?

On November 2, 2026, we determined that some of your information may have been involved in an incident involving unauthorized access to certain employee accounts. We immediately engaged outside counsel and a leading cybersecurity firm to investigate. The investigation determined that an unauthorized third party gained access through social engineering. With that access, the unauthorized third party was able to download certain files. We took steps to contain the incident, including revoking the compromised accounts' access. The investigation found no ongoing evidence of any unauthorized activity. Following the investigation, Dexcom reviewed the affected files and determined that your information may have been involved.

What Information Was Involved?

Based on our investigation to date, the information that may have been involved includes one or more of the following: your name, address, and health information that could include your preferred pharmacy, your healthcare provider, your date of birth, prescription number, certain diagnoses, and other limited health information, such as an indication that you are a Dexcom user. The incident did not involve your Social Security number, credit or debit card numbers, or other financial information.

What We Are Doing

We are committed to protecting your personal information. To do so, we will continue to review, audit, and improve our controls and processes. Upon learning of the incident, we engaged, through counsel, a leading cybersecurity firm to investigate and determine the details and scope of the incident and what personal information may have been impacted. We also took steps to contain the incident, including revoking the compromised accounts' access, and we have reinforced our security awareness training to help prevent similar incidents. We have no indication that any of your information has been misused.

What You Can Do

Information on what you can do is provided in the attachment to this letter, including the Steps You Can Take to Protect Your Data, which provides guidance on further protecting your personal information.

For More Information

If you have any questions about this incident, please call (844) 971-8641, Monday through Friday, between 8:00 a.m. and 5:30 p.m. Central Time, excluding major U.S. holidays.

STEPS YOU CAN TAKE TO PROTECT YOUR DATA

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-888-378-4329	Phone: 1-888-397-3742	Phone: 1-800-916-8800
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission, local law enforcement, and/or the Attorney General's office in your state. You can obtain information from these sources, as well as the credit reporting agencies listed above, about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. You should obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information follows for the Federal Trade Commission, as well as certain state Attorney General Offices that we are required to provide pursuant to state law. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov, 1-888-743-0023.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583/1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and the New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, please contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If a creditor can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, please contact each of the credit reporting agencies at the addresses below, also provided in the chart above:

Experian Security Freeze, P.O. Box 9554, Allen, TX 75013, www.experian.com

TransUnion Security Freeze, P.O. Box 2000, Chester, PA 19016, www.transunion.com

Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

You will need to supply your name, address, date of birth, Social Security number, and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save time by lifting the freeze only at that particular credit bureau. Otherwise, you will need to make the request with all three credit bureaus.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report or report any suspected identity theft to your state Attorney General.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act ("FCRA") promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.