SEATAC ELECTRIC

12/6/2024

NOTICE OF DATA BREACH

To All Employees,

We are writing to tell you about a situation that may have exposed some of your personal information. We take the protection of your information very seriously and are contacting you to explain the circumstances, steps we are taking in response and resources we are making available to you.

What Happened? On 12/4/2024, we experience a cyber event that may have resulted in an employee's email account being compromised. According to Microsoft, it is impossible to determine whether any data was downloaded during the intrusion.

What Information Was Involved? Information that may have been available includes employee names, contact information, Social Security numbers, dates of birth, home addresses, salary information, benefits elections and insurance policy information, medical information and other related information maintained for HR purposes, but only to the extent it was the topic of an email exchange involving the email account in question.

What We Are Doing. Immediately upon discovering the attack, we initiated response protocols, activated our technical team and hardened our defenses against unauthorized activity, including reaching out to experts at Microsoft. We have also notified local law enforcement and the Washington State Attorney General's Office.

We will continue to provide regular reminders and training for employees on how to spot and avoid being victimized by suspicious emails leading to malware/ransomware events in the future. Cybercriminals will continue to find new ways to target company employees, and we must all continue to be vigilant against increasingly sophisticated schemes. Additionally, we have taken additional security measures to strengthen our network against similar incidents in the future.

What You Can Do. We want to make sure you are aware of steps you may take to guard against potential identity theft or fraud. The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year. Contact information is as follows:

Equifax: equifax.com/personal/credit-report-services or 1-800-685-1111
Experian: experian.com/help or 1-888-397-3742
TransUnion: transunion.com/credit-help or 1-888-909-8872

SEATAC ELECTRIC

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft.

If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, to the Washington Attorney General, the Oklahoma Attorney General and/or to the Federal Trade Commission (FTC).

To contact the Washington Attorney General, go to www.atg.wa.gov or call 1-800-551-4636. To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Security Freeze
You also have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency.

In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources on Identity Theft

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can also be found on the FTC's website at: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.]

We are providing this notice out of an abundance of caution because your information was available and potential access to or acquisition of that information, before the system was locked down, could not be definitively ruled out.

Respectfully,
Tom Jordan
President