June 27, 2018

Dear Current or Former EBMUD Employee:

Staff identified a potential breach of data housed within Marconi, the District's emergency response software. Given this potential breach, and the possibility that some limited employee information was exposed, we are reaching out to you with incident details. This notice is being provided to individuals employed by the District between February 5, 2014 and June 4, 2018.

First, securing and protecting our employees' confidential information is a top priority for the District and it is a responsibility that we take very seriously. We value our relationship with our customers and employees, and respect everyone's right to privacy. This is why, as a precautionary measure, we are informing you of this incident and the potential exposure of some limited employee information.

This notice describes what happened, what we have done in response, and steps that you can take to help protect your information.

**What Happened:** On May 25, 2018, staff learned that unauthorized individuals may have accessed ersquared.org, the third-party hosting environment for Marconi. Upon this discovery, staff, in conjunction with the Multi-State Information Sharing and Analysis Center (MS-ISAC), immediately began investigating the system to determine what happened and what District information may have been affected. Although there is no evidence that personal information was accessed or that any other District systems were compromised, the District is notifying you as a precaution. The period during which employee information may have been accessed is February 5, 2014 through June 4, 2018.

**What Information Was Involved:** The Marconi application database held some employee information, specifically: name, employee identification number, work email address, job title, and Marconi password hash (encrypted). As an emergency notification system, select employees had provided personal email address, home address, home phone number, and mobile phone number.

**What We Are Doing:** We are committed to protecting customers' and employees' privacy. Once the nature of the access was identified, the District removed Marconi from service on June 4, 2018 and is working to build a stronger and more secure hosting environment for the application. Part of this effort includes decreasing the amount of personal information held by the system. Marconi will not be brought back into service until that effort is complete.

Furthermore, the District will increase its efforts to monitor other third-party hosted systems to ensure they comply with the District's security expectations. The District will also work to enhance vendor security safeguards, procedures, and practices with respect to District data, reducing the likelihood and impact of any future incidents. Staff works hard to balance adding new applications and web enabled technologies with security of employee and customer data.

**What You Can Do:** Although there is no evidence your Marconi password was compromised, if you used your Marconi password on any other systems, you should change it as soon as possible on those other systems as a precaution. Current employees will receive an email requesting a District password change ahead of the standard 6-month password rotation schedule. That email will contain instructions regarding each password that must be changed (for example, Windows/computer login and Oracle/ETS, GWO, etc). If you reset your passwords since June 4, 2018, no additional change will be required. As a general practice, security experts advise using unique, strong, and complex passwords for all services you use. This includes personal, non-District related accounts. Avoid using the same password on different web sites.

**Other Important Information:** For additional information about privacy rights, visit the website of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov. For general tips regarding managing your personal information, visit the California Office of the Attorney General’s “Breach Help: Tips for Consumers” website https://www.oag.ca.gov/privacy/other-privacy/breach-help-tips-for-consumers.

**For More Information:** Please see the attached FAQ for answers to questions you may have regarding this notice. If you have additional questions about this incident, please contact the Help Desk at (510) 287-0235 or helpdesk@ebmud.com.

The District understands the importance of your personal information, and sincerely apologizes for any inconvenience this incident may cause.

Sincerely,

Alexander R. Coate
General Manager