**South Whidbey Fire & EMS**

**Notice Regarding Data Security Incident**

The privacy and security of the personal information we maintain is of the utmost importance to at South Whidbey Fire & EMS (“SWFE”). We want to provide individuals with information about a data security incident that has affected our organization, and let you know that we continue to take significant measures to protect individual personal information. SWFE discovered suspicious activity in one of our employee email accounts. Upon learning of the issue, we commenced a prompt and thorough investigation.

As part of the investigation, we engaged leading third-party cybersecurity professionals experienced in handling these types of incidents. The investigation worked to identify what individual information, if any, might have been accessed by an unauthorized third-party. After an extensive forensic investigation and comprehensive manual review of all the data impacted, on February 2, 2023, we discovered that certain personal information within the email environment was potentially accessed by an unauthorized party from April 21, 2022 through May 21, 2022.The information involved includes individual name, date of birth, Social Security Number, driver license number, financial account number, passport number, payment card number, username or email address and password, and certain personal health information. **The information involved belongs to current or former employees or volunteers only.**

SWFE has no evidence that the information involved was or will be specifically misused. However, out of an abundance of caution, SWFE is notifying affected individuals via mail about the incident, and including in the communication steps individuals may take to protect the privacy of their personal information.

Involved individuals are encouraged to take steps to protect themselves against identity fraud, including placing a fraud alert/security freeze on their credit files, obtaining free credit reports, and remaining vigilant in reviewing financial account statements and credit reports for fraudulent or irregular activity on a regular basis. Involved individuals may obtain additional ways to protect their information below.

The security and privacy of personal information is of the utmost importance to SWFE. SWFE continually evaluates and modifies its practices to enhance the security and privacy of personal and health information, and is taking measures to augment its existing cybersecurity

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 866-674-3884. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against misuse of your information. The response line is available Monday through Friday, 6:00AM – 3:30PM Pacific Time, excluding holidays.

**– OTHER IMPORTANT INFORMATION –**

**Placing a Fraud Alert**

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

|  |  |  |
| --- | --- | --- |
| ***Equifax***  P.O. Box 105069  Atlanta, GA 30348-5069  <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>  (800) 525-6285 | ***Experian***  P.O. Box 9554  Allen, TX 75013  <https://www.experian.com/fraud/center.html>  (888) 397-3742 | ***TransUnion***  Fraud Victim Assistance Department  P.O. Box 2000  Chester, PA 19016-2000  <https://www.transunion.com/fraud-alerts>  (800) 680-7289 |

**Consider Placing a Security Freeze on Your Credit File**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

|  |  |  |
| --- | --- | --- |
| ***Equifax Security Freeze***  P.O. Box 105788  Atlanta, GA 30348-5788  <https://www.equifax.com/personal/credit-report-services/credit-freeze/>  (888)-298-0045 | ***Experian Security Freeze***  P.O. Box 9554  Allen, TX 75013  <http://experian.com/freeze>  (888) 397-3742 | ***TransUnion Security Freeze***  P.O. Box 160  Woodlyn, PA 19094  <https://www.transunion.com/credit-freeze>  (888) 909-8872 |

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information.  After receiving your freeze request, each credit reporting company will send you a confirmation letter containing 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.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

**Obtaining a Free Credit Report**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

**Additional Helpful Resources**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

###