BRADLEY BERNSTEIN SANDS

Darin Sands
Portland Office

T 971-998-4751
dsands@bradleybernsteinllp.com
bradleybernsteinllp.com

April 26, 2021

Re: Notice of Data Event

To the Office of the Attorney General:

We represent the Seattle Police Officers' Guild ("SPOG") in connection with a data security incident that impacted 1297 of its members and former members who are believed to be Washington residents, all of whom have been notified of the incident. This letter serves as notice to the Attorney General.

Nature of the Incident

On March 30, 2021, SPOG was notified that it was one of the more than the 30,000 organizations in the United States whose Microsoft Exchange email servers were potentially targeted by a malicious actor seeking to gain access to its email systems. Impacted information was exposed between March 6, 2021, and March 30, 2021.

Upon learning of the vulnerability, SPOG immediately took the impacted server offline and began working with IT professionals and law enforcement to ensure that no additional security vulnerabilities exist.

This incident only affected SPOG's email server—its data server was not impacted. At this point, there is no evidence indicating that any other systems were impacted by the attack.

SPOG is actively working with federal and state law enforcement to investigate the incident. As of now, there is no reason to believe that SPOG was specifically targeted. Nor is there any evidence that any information contained on the SPOG email server has been distributed or made available to any third party.

Number of Washington Residents Impacted

1297 members were impacted and notified of the incident on April 6, 2021, by letter or by email. A sample of the notification is attached to this letter as Exhibit A.

Personal Information Impacted

The data accessed included emails and personal information such as names, personal and work email addresses, physical addresses, dates of birth, and in some cases social security numbers.

BRADLEY BERNSTEIN SANDS

Response to Incident

SPOG has been working closely with its local and federal law enforcement partners and its IT professionals to investigate the incident and to implement additional security measures designed to prevent a recurrence of such an attack and to protect those impacted.

SPOG is providing LifeLock to all individuals impacted.

Additionally, SPOG has held informational sessions/workshops with cyber security professionals to assist with taking follow up steps to protect personal data.

Follow Up

If you have any questions or require additional information, please contact me at dsands@bradleybernsteinllp.com or 971.998.4751.

Best Wishes,

Darin Sands
Bradley Bernstein Sands LLP

Exhibit A

Seattle Police Officers' Guild
2949 Fourth Avenue South
Seattle, WA 98134
206.767.1150
www.seattlepoliceofficers.com

Mike Solan – President
Dan Auderer– Vice President
Walt Hayden – Secretary/Treasurer

NOTICE OF DATA BREACH

Dear Current, Former SPOG and SPMA Members;

As many of you were notified last week in our general membership meeting, SPOG experienced a data breach of our email sever.

WHAT HAPPENED?

On March 30, 2021, we were notified that we were one of the more than the 30,000 organizations in the United States whose Microsoft Exchange email servers were potentially targeted by a malicious actor seeking to gain access to our email systems.

Upon learning of the vulnerability, we immediately took the impacted server offline and we have been working with our IT professionals to ensure that no additional security vulnerabilities exist.

This breach only affected our email server, our data server was not impacted. At this point, there is no evidence indicating that any other systems were impacted by the attack.

We are also actively working with federal and state law enforcement to investigate the breach. As of now, we have no reason to believe the Seattle Police Officers' Guild was specifically targeted. Nor have we seen any evidence that any information contained on our email server has been distributed or made available to any third party.

WHAT INFORMATION WAS INVOLVED?

The data accessed included emails and personal information such as names, personal and work email addresses, physical addresses, dates of birth, and in some cases social security numbers.

Our IT professionals have identified the following timeline of when this breach occurred. The initial breach occurred on March 6th and was remediated on March 30th, 2021.

WHAT WE ARE DOING

We have been working extensively with our IT professionals along with local and federal law enforcement partners. With their guidance we have also implemented additional security measures designed to prevent a recurrence of such an attack and to protect those impacted by this breach.

SPOG will be providing free LifeLock to all current and former SPOG and SPMA Members whose data was compromised.

Additionally, SPOG will be holding informational sessions/workshops with cyber security professionals to assist you with these security protocols (social distancing measures will be adhered). The first sessions are on Thursday, 4/8 at 0800 and 1300 at the SPOG Office. These are open to all those impacted by this breach.

Seattle Police Officers' Guild
2949 Fourth Avenue South
Seattle, WA 98134
206.767.1150
www.seattlepoliceofficers.com

WHAT YOU CAN DO

Review the attachment to this letter (Steps You Can Take to Further Protect Your Information).
Sign up for LifeLock.
Attend SPOG informational sessions/workshops.

FOR MORE INFORMATION

For further information and assistance, please contact the SPOG Office at mail@seattlepoliceguild.org.

Sincerely,

Mike Solan
President

Seattle Police Officers' Guild
2949 Fourth Avenue South
Seattle, WA 98134
206.767.1150
www.seattlepoliceofficers.com

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. 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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (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.

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

We recommend also placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Seattle Police Officers' Guild
2949 Fourth Avenue South
Seattle, WA 98134
206.767.1150
www.seattlepoliceofficers.com

Mike Solan – President
Dan Auderer– Vice President
Walt Hayden – Secretary/Treasurer

Norton LifeLock Identity Protection

In addition, we have arranged with Norton LifeLock to provide you with identity theft protection services for two years, at no cost to you. The package provides you with the following benefits:

Primary Identity Alert System
24/7 Life Support at a SPOG only call-center
U.S. Based Identity Restoration Specialists
Million Dollar Protection Package
90 Day subscription to Norton Security Deluxe
Dark Web Monitoring
Credit, Bank, Utility Account Freezes
USPS Address Change Verification
Fictitious Identity Monitoring
Credit, Checking and Savings Account Alerts
Three Bureau Credit Monitoring

To take advantage of this offer, you must enroll within 100 days from receipt of this letter.

Enrollment Instructions will be sent in a separate email by 4/9/21

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338) or visit www.atg.wa.gov/credit-freeze-fraud-alerts

Security Freeze

In Washington, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.