Jeff Boogay
Office: 267-930-4784
Fax: 267-930-4771
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

March 19, 2019

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
Email: securitybreach@atg.wa.gov

Re: Notice of Data Security Incident

Dear Sir or Madam:

Our firm represents the Seattle Housing Authority ("SHA") and writes to supplement our notice provided to your office on February 22, 2019 of an incident that may affect the privacy of some personal information relating to six hundred eighty-seven (687) Washington residents. By providing this notice, SHA does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

Nature of the Data Event

On or around January 7, 2019, SHA became aware of a break-in at the office of one of its housing developments. SHA immediately contacted law enforcement and launched an investigation into the incident which determined that the actor(s) stole a laptop computer used by SHA to process rent payments. The investigation determined that the files on the computer contained certain personal information related to residents at the SHA housing development, which includes the following information related to Washington residents: name, bank account number, and routing number.

Notice to Washington Residents

Since discovering this incident, SHA has been working diligently to confirm the nature and scope of the event, determine which individuals may have been affected, and determine contact information for those individuals. On March 19, 2019, SHA is mailing written notice of this incident to potentially affected individuals, which includes six hundred eighty-seven (687) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the break-in and theft, SHA immediately took steps to investigate and respond to the incident, including the involvement of law enforcement. SHA also took steps to identify the individuals affected, the types of information affected and their addresses. SHA has been working diligently to ensure

the security of its facilities, determine the full nature and scope of the event, and identify potentially affected individuals. While SHA has extensive measures in place to protect the information in its care, it is working to implement additional safeguards to protect the security of its facilities and information.

Additionally, while to date, the investigation has found no evidence of actual or attempted misuse of personal information potentially affected by this event, in an abundance of caution, SHA is providing potentially impacted individuals with notice of this event. SHA is also providing potentially impacted individuals with guidance on how to protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and explanation of benefits form and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. SHA will also be providing notice of this event to other state regulators as required by law.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,

Jeff Boogay of
MULLEN COUGHLIN LLC

JB/ajd
Enclosure

EXHIBIT A

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<LastName>>,

We are writing to inform you of a recent event that may affect the security of some of your personal information. While there is currently no evidence that your information has been misused, we are providing you with information regarding the incident, and the steps that are being taken in response.

On or around January 7, 2019, Seattle Housing Authority ("SHA") became aware of a break-in at the office at their NewHolly housing development. SHA immediately launched an investigation into the incident and determined that a laptop used in the processing of rent payments was stolen from the facility. SHA immediately contacted police and are cooperating with their investigation, as well as continuing their own.

The investigation determined that the specific laptop taken in the theft may contain certain information pertaining to current and former residents of the NewHolly housing development. If you paid your rent with a money order, none of your information was stored on the stolen laptop, and there is no risk of disclosure. However, if you paid your rent with a check , while SHA currently has no evidence that your information was subject to attempted misuse, SHA believes that your name, bank account number, and routing number were contained in files on the stolen laptop.

The confidentiality, privacy, and security of information in SHA's care is one of their highest priorities. Upon learning of this incident, SHA immediately took steps to re-secure the facility and notify law enforcement. SHA also took steps to identify what information was contained on the stolen laptop. Please know that SHA has an ongoing commitment to maintaining a high level of security of their facilities and the information in their care. While SHA has no evidence of any actual attempted misuse of any of the information contained on the laptop, as a precaution SHA is partnering with a company called Kroll to offer individuals access to one (1) year of free identity monitoring services. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

*You have until **June 15, 2019** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

As a best practice, SHA recommends you review your bank accounts for any suspicious activity, and if you feel it appropriate, contact your financial institution to alert them regarding this letter. Additionally, SHA encourages you to review the attached "Steps You Can Take to Protect Against Identity Theft and Fraud", as a matter of best practices should you note any suspicious activity with your accounts. Again, if you paid with a money order, your information was not contained on the laptop.

SHA understands you may have questions about this incident. Please feel free to reach out to us at 206-615-3302 or via email at cindy@seattlehousing.org.

SHA takes the security of their facilities and the privacy of information that you entrusted to them very seriously. SHA sincerely regrets any inconvenience or concern this incident may cause you.

Sincerely,

Cindy Sribhibhadh
Property Management Administrator

Steps You Can Take to Protect Against Identity Theft and Fraud

While we have no evidence in this case of any actual access to or attempted misuse of any information on the stolen laptop, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.