BakerHostetler

Baker&Hostetler LLP

1170 Peachtree Street
Suite 2400
Atlanta, GA 30309-7676

T 404.459.0050
F 404.459.5734
www.bakerlaw.com

John P. Hutchins
direct dial: 404.946.9812

July 21, 2020

**VIA E-MAIL (SECURITYBREACH@ATG.WA.GOV)**

Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104

*Re: Incident Notification*

Dear Sir or Madam:

I am writing to notify you of a data security incident on behalf of my client, City Ministries, a social service organization based in Kirkland, Washington, whose mission is to serve the community with faith-based volunteerism and resources.

City Ministries recently concluded its investigation of a data security incident that involved unauthorized access to the email account of a City Ministries employee. Upon learning of the incident, City Ministries immediately secured the email account and launched an internal investigation with the assistance of a cyber security firm that was engaged to assist outside legal counsel.

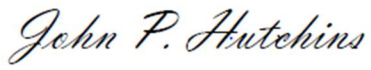
As part of the investigation, City Ministries conducted a comprehensive review of the emails and attachments in the email account to identify individuals whose information may have been involved in this incident. Through the investigation, City Ministries determined that an unauthorized party accessed the employee's email account on February 11, 2020. The investigation was unable to rule out the possibility that the unauthorized party may have been able to access emails and attachments in the account. In an abundance of caution, City Ministries reviewed the emails and attachments in the account to identify individuals whose information may have been accessible to the unauthorized person. On May 1, 2020, City Ministries determined that the name, Social Security number, date of birth, driver's license number, financial account information and/or credit card information and email and password information of 533 Washington residents were contained in the emails and attachments in the account.

On July 21, 2020, City Ministries will mail notification letters via United States Postal Service First-Class mail to the residents whose information may have been involved in this incident, in accordance with Wash. Rev. Code § 19.255.010. A copy of the notification letter is enclosed. City Ministries is offering one year of complimentary credit monitoring and identity theft protection service through Kroll to the individuals whose Social Security or driver's license number was in the accessed accounts. City Ministries has also established a dedicated call center where all individuals may obtain more information regarding the incident.

To help prevent something like this from happening again, City Ministries is taking steps to enhance its existing security protocols and re-educating its staff about these types of incidents.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



John P. Hutchins
Partner

Enclosure

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

We write to inform you that we identified and addressed a security incident that may have involved some of your information. This letter explains the incident, measures we have taken, and steps you can take in response.

On February 11, 2020, a City Ministries employee clicked on a link in an email that turned out to be part of a phishing scam. As a result, an unknown unauthorized individual obtained access to the employee's email account. This unknown individual then sent approximately 1,600 emails from the employee's account, which prompted Microsoft to shut down the email account.

Upon learning of this phishing incident, we immediately took steps to secure all of City Ministries' email accounts, reset passwords, retained outside counsel and launched an investigation. A third-party cybersecurity firm was engaged by our counsel on our behalf to further assist the investigation.

We have concluded that investigation. On May 1, 2020, we confirmed that an email or an email attachment in the employee's email account contained your <<b2b_text_1(ImpactedData)>>. Although we have no evidence that any of your information has been misused, we wanted to let you know that this incident occurred.

We are also offering you a complimentary one-year membership in identity monitoring services through Kroll. This service helps detect possible misuse of your personal information and provides you with complimentary identity monitoring services including Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Activating this program will not hurt your credit score. For more information on Kroll's monitoring services, including instructions on how to activate your complimentary membership, as well as some additional steps that you can take to help protect yourself, please see the additional information provided with this letter.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **[Date]** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

We encourage you to take advantage of the identity monitoring services being offered. We also encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your free credit reports for any unauthorized activity. You should review your financial account statements closely and report any unauthorized activity immediately.

Your confidence and trust are important to us, and we regret any inconvenience or concern this may cause. To help prevent a similar incident in the future, we are taking steps to enhance our existing security protocols and re-educating our staff for awareness on these types of incidents. If you have any questions, please call our dedicated call center at 1-844-958-2769 Monday through Friday from 8:00 am to 5:30 pm Central Time.

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Centre, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one (1) year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com.
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com.
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com.

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 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.); and
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Kroll | A Division of DUFF & PHELPS

## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

### Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
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.