LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720-292-2052

October 20, 2019

VIA ELECTRONIC SUBMISSION

NH Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301
Email: attorneygeneral@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent Youth For Christ USA, Inc. ("YFC") in connection with a recent data security incident, which is described in greater detail below. YFC is a non-profit organization, headquartered in Englewood, Colorado, which provides faith-based services and programs to youths across the country. This incident potentially impacted the personal information of one (1) New Hampshire resident.

1. Nature of the security incident.

On July 30, 2019, YFC discovered unusual activity within its email system. Upon discovering this activity, YFC immediately took measures to secure its system and all YFC email accounts. YFC also launched an investigation and engaged a leading, independent forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. On August 15, 2019, YFC received the preliminary results of the investigation which indicated that an unauthorized individual had gained access to some YFC employee email accounts. Upon learning this information, YFC commenced a data review project, with the assistance of the forensics firm, to determine whether the YFC email accounts at issue contained personal information as defined under applicable state law. On September 18, 2019, the results of the data review project revealed that those email accounts contained personal information of one New Hampshire resident which may have been accessed without authorization.

The information potentially impacted as a result of this incident may have included the notified individual's name, Social Security number, date of birth, and employee identification number.

2. Number of New Hampshire residents affected.

YFC notified one New Hampshire resident regarding this incident, whose information was contained within the accessed email accounts referenced above. Notification letters were mailed on October 16, 2019. A sample copy of the letter sent to potentially impacted individuals is enclosed.

3. Steps taken relating to the incident.

YFC has taken steps in response to this incident to enhance the security of personal information in its possession in an effort to prevent similar incidents from occurring in the future, including updating its policies and procedures regarding the organization's internal and external means of transferring personal information. YFC has also taken steps to implement multi-factor authentication for those departments within its organization that are primarily responsible for handling personal information. In addition, YFC notified the Federal Bureau of Investigation of this incident and will provide any assistance necessary to hold the perpetrators if this incident accountable. Furthermore, YFC has offered affected individuals twelve (12) months of complimentary credit monitoring, fraud consultation, and identity theft monitoring services through Kroll.

4. Contact information.

YFC remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (720) 292-2052, or by e-mail at Alyssa.Watzman@lewisbrisbois.com.

Best regards,

/s/ Alyssa Watzman

Alyssa Watzman
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure

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

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

Subject: Notification of Data Security Incident

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

We are writing to inform you of a data security incident experienced by Youth For Christ USA, Inc. ("YFC") that may have affected some of your personal information. The privacy and security of your information is extremely important to us. That is why we are writing to inform you of this incident, to advise you of steps that can be taken to help protect your information, and to offer you twelve (12) months of complimentary identity monitoring services.

What Happened? On July 30, 2019, we discovered unusual activity within the YFC email system. Upon discovering this activity, we took immediate steps to secure all YFC email accounts. We also launched an investigation and engaged a leading forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. On August 15, 2019, as a result of this investigation, we learned that an unauthorized individual gained access to some YFC employee email accounts. On September 18, 2019, we learned that those email accounts contained some of your personal information which may have been viewed by an unauthorized individual.

Please note that this unauthorized access was limited to information transmitted via email and did not affect any other information systems. Importantly, we are not aware of the misuse of any of your personal information.

What Information Was Involved? The information potentially impacted as a result of this incident may have included your <<ClientDef1(Data Sets)>><<ClientDef2(Data Sets)>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. In addition, because we take the security of all information that we have in our systems very seriously, we have also taken steps to enhance the security of our email system in order to minimize the likelihood of similar incidents occurring in the future. In addition, we reported this matter to the Federal Bureau of Investigation and will provide whatever assistance is necessary to hold the perpetrators of this incident accountable. Finally, while we are not aware that any potentially impacted information has been misused, we are offering you complimentary identity monitoring services for twelve (12) months through Kroll, a global leader in risk mitigation and response. These services include: Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

What You Can Do: We recommend that you activate your complimentary Kroll services. Activation instructions and a description of the services provided are included with this letter. We also recommend that you review the guidance provided on the next page about how to help protect your personal information.

For More Information: Further information and resources regarding the protection of your personal information appear on the following pages. If you have questions or need assistance, please call Kroll at 1-866-775-4209 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major US holidays. Kroll representatives are fully versed on this incident and can answer any questions that you may have regarding the protection of your personal information.

We take your trust in us and this matter very seriously and we apologize for any worry or inconvenience that this incident may cause you.

Sincerely,

Sean Wallinger
Vice President of Finance
Youth for Christ USA, Inc.

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, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may 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 print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one (1) year. 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.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Kroll | A Division of DUFF&PHELPS

As referenced above, we have secured the services of Kroll to provide identity monitoring services at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services include[1] Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Services

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services. You have until January 8, 2020 to activate your identity monitoring services.

Membership number: **<<Member ID>>**

If you have questions, please call 1-866-775-4209, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Take Advantage of Your Services

You've been provided with access to the following services 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.