Winget | Spadafora | Schwartzberg | LLP

1993-2018 25 years

NEW YORK:
45 Broadway
32nd Floor
New York, NY 10006
T 212.221.6900
F 212.221.6989
McCarthy.D@wssllp.com

August 20, 2019

VIA REGULAR MAIL
Attorney General Gordon McDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Dear Attorney General McDonald:

Our firm represents Christian Investors Financial, Inc. in connection with a suspected data breach. Pursuant to N.H. Rev. Stat. Ann. § 359-C:20, we write to notify you of an incident that may have potentially affected two (2) New Hampshire residents.

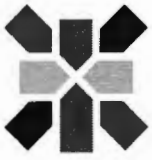
On May 14, 2019, we became aware of suspicious activity in the email account of one of our employees. We immediately acted to shut down unauthorized access and further tightened security over the email account. We contracted with a third-party forensic firm to investigate the incident. The forensic firm identified that this employee's email account had been compromised between April 23, 2019 and May 14, 2019. No other email accounts or systems appear to have been affected. However, the affected email account does receive incoming faxes, certain voicemails and emails sent to our service@christianinvestors.org address. Upon completion of the forensic investigation we further contracted with third-party experts to review the email account for content and/or attachments that may contain personally identifiable information. Information contained in the email account may have included names, Social Security numbers, dates of birth, driver's license or state ID numbers, financial account numbers, username and initial passwords, and email addresses.

We are in the process of notifying all affected New Hampshire citizens of this incident in the form attached hereto.

Please feel free to contact me if we can provide you with any additional information.

Very truly yours,

/s/Dianna McCarthy
Dianna D. McCarthy



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF EMAIL INCIDENT

Dear <<Name 1>>:

We are writing to you because of an email security incident that may involve your personal information associated with Christian Investors Financial. Although we are unaware of any actual misuse of your personal information, we are providing notice to you about the incident. We take the privacy and protection of your personal information very seriously and highly recommend you carefully review the information contained in this letter to best protect yourself in the future.

What Happened? On May 14, 2019, we became aware of suspicious activity in the email account of one of our employees. We immediately acted to shut down unauthorized access and further tightened security over the email account. We contracted with a third-party forensic firm to investigate the incident. The forensic firm identified that this employee's email account had been compromised between April 23, 2019 and May 14, 2019. No other email accounts or systems appear to have been affected. However, the affected email account does receive incoming faxes, certain voicemails and emails sent to our service@christianinvestors.org address. Upon completion of the forensic investigation we further contracted with third-party experts to review the email account for content and/or attachments that may contain personally identifiable information. Out of an abundance of caution, we are notifying everyone who may have sent or received personally identifiable information to or from the affected email account.

What Information Was Involved? Information contained in the email account may have included names, Social Security numbers, dates of birth, driver's license or state ID numbers, financial account numbers, username and initial passwords, and email addresses.

What We Are Doing? Cyber-attacks continue to increase and evolve. For this reason, and to help prevent this type of incident in the future, Christian Investors Financial is actively enhancing data security procedures. We have implemented security measures designed to prevent a recurrence of such an attack, to protect privacy of Christian Investors Financial's valued clients and employees, and other cybersecurity layers of protection. We are currently in the process of communicating with all necessary entities.

What You Can Do? Please review the Privacy Safeguards on the following page for additional information on how to better protect against identity theft and fraud.

For More Information. We have retained Epiq Corporate Services, Inc. ("Epiq") to assist with our notification and answer questions you may have. We sincerely regret any inconvenience or concern this matter may cause you. If you have questions or need assistance, please call 877-204-9532 from 6:00 am to 6:00 pm Pacific Time, Monday through Friday.

We sincerely regret that this unfortunate incident occurred. We are committed to protecting your personal information and we hope this information will be useful to you.

Sincerely,

Scott Achterling,

Chief Operating Officer
Christian Investors Financial

Complimentary Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, three-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<<Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Privacy Safeguards

- **Never email confidential information** unless done via a secured email system. Christian Investors has had a document exchange portal available since late 2017 at https://christianinvestors.leapfile.net/ for submitting documents in a more secure environment. Please use it when sending documents containing personal identifiable information such as Social Security numbers, dates of birth, driver's license or state ID numbers, usernames and financial account numbers.
- **Change your passwords** on any accounts that may have been compromised and remember to use unique passwords across different accounts.
- **Remain vigilant and monitor your credit and identity** by reviewing your account statements and monitor credit reports for any unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.
- **Keep an eye on your financial accounts** by visiting your online bank and financial accounts, and setting up any alert features they may have. This may keep you notified of any unusual activity, should it occur.
- **Report** any suspected incidents of identity theft to local law enforcement, your state's attorney general, or the Federal Trade Commission.
- **Place a Security Freeze** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. In order to request a security freeze, you may need to provide all 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;

You also have the right to issue a fraud alert which will warn lenders that you may have been a fraud victim. When you request a fraud alert be added with any of the three major credit bureaus, the bureau you contacted will notify the other two and alerts will be added with those bureaus as well. This extra precaution will notify any potential lenders that they should contact you before granting any new line of credit in your name. This fraud alert will stay on your credit report for 1 year, and you can renew the fraud alert when it expires.

Other Important Information

You can also obtain additional information from the Federal Trade Commission and the three major credit reporting bureaus about fraud alerts and security freezes. You may contact the three major credit bureaus via the following addresses, toll-free telephone numbers, and websites:

Equifax Fraud Reporting
1-888-548-7878
P.O. Box 105069
Atlanta, GA 30348-5069
www.alerts.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

You may contact the Federal Trade Commission at:

Federal Trade Commission
Identity Theft Clearinghouse
600 Pennsylvania Ave., NW
Washington, DC 20580
1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261
www.consumer.gov/idtheft