

RECEIVED

APR 03 2018

CONSUMER PROTECTION

March 30, 2018

Kevin M Scott
312.821.6131 (direct)
Kevin.Scott@wilsonelser.com

Attorney General Joseph A. Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General Foster:

We represent Cross Road Health Ministries, Inc. ("CRHM"), a not-for-profit faith based ministry committed to providing health care services, with its corporate offices located in Glennallen, Alaska and locations throughout Alaska, with respect to a recent data security incident described in more detail below. CRHM takes the security and privacy of the information in its control very seriously, and is taking steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

On January 17, 2018, CRHM discovered that a purported technical support company that on several occasions was allowed to connect remotely to its computer network for the purpose of resolving computer software issues, was part of a fraudulent scamming operation. CRHM immediately took action and engaged forensics experts to conduct an investigation and determine what information was at risk of compromise during the unauthorized access to its network. CRHM determined that during a purported support session, a file containing some of its employees' personal information associated with payroll may have been accessible, which may have included their name, date of birth, Social Security number, and financial account information used for direct deposit. CRHM has reported this incident to law enforcement.

2. Number of New Hampshire residents affected.

One (1) resident of New Hampshire was affected by this security incident. A notification letter to this individual was mailed on March 30, 2018 via first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken relating to the incident.

CRHM has taken steps to prevent a similar event from occurring in the future. Those steps include providing training to employees to identify and intercept fraudulent activity, limiting employee vendor engagement to a list of acceptable vendors and reviewing its policies and procedures. CRHM has also

provided all potentially affected individuals with 12 months of complimentary credit monitoring and identity theft restoration services.

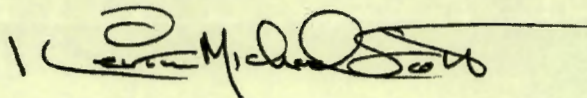
4. Contact information.

CRHM remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (312) 821-6131 or Kevin.Scott@wilsonelser.com.

Please let us know if you have any questions.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Kevin M. Scott

Enclosure



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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>>,

We are writing to inform you of an incident at Cross Road Health Ministries, Inc (formerly Cross Road Medical Center) that may have resulted in the disclosure of some of your personal information including your name and Social Security number ("SSN"). We take the security of your personal information very seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains information about what happened, steps we have taken and resources we are making available to you to protect your identity.

On January 17, 2018, we discovered that a purported technical support company that on several occasions was allowed to connect remotely to our computer network for the purpose of resolving computer software issues, was part of a fraudulent scamming operation. We immediately took action and engaged forensics experts to conduct an investigation and determine what information was at risk of compromise during the unauthorized access to our network. We determined that during a purported support session, a file containing some of your personal information associated with payroll may have been accessible, which may have included your name, date of birth, Social Security number, and financial account information used for direct deposit. We have no evidence of misuse of your information and have reported this incident to law enforcement.

In an abundance of caution, we have secured the services of Kroll to provide identity monitoring, 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 identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

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

You have until June 28, 2018 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.

We take the security of all information in our systems very seriously, and want to assure you that we are taking steps to prevent a similar event from occurring in the future. Those steps include providing training to employees to identify and intercept fraudulent activity, limiting employee vendor engagement to a list of acceptable vendors and reviewing our policies and procedures.

We sincerely regret any inconvenience that this matter may cause you, and remain dedicated to protecting your information. Please see the addendum for additional steps you can take to protect your personal information. If you have any questions, please call 1-866-775-4209, Monday through Friday, 5:00 a.m. to 2:00 p.m., Alaska Time.

Sincerely,

Joel Medendorp
CEO

Cross Road Health Ministries, Inc (formerly Cross Road Medical Center)

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina:

It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the nationwide three credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

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

For residents of Massachusetts:

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

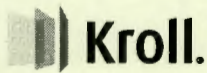
Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a small fee to place, lift, or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ 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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.