

BakerHostetler

RECEIVED

NOV 04 2019

CONSUMER PROTECTION

Baker&Hostetler LLP

Key Tower
127 Public Square, Suite 2000
Cleveland, OH 44114-1214

T 216.621.0200
F 216.696.0740
www.bakerlaw.com

David E. Kitchen
direct dial: 216.861.7060
dkitchen@bakerlaw.com

November 1, 2019

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of Canto, Rausch, Deck & Co., P.A. ("Canto Rausch") to notify you of a security incident involving one New Hampshire resident.

Canto Rausch's investigation into an email phishing incident recently determined that an unauthorized individual may have gained access to a small number of employee email accounts. Upon first learning of the incident, Canto Rausch took immediate steps to secure all its email accounts. Canto Rausch also began an investigation with the assistance of a cybersecurity firm to determine what happened, who was impacted and what information may have been affected. The investigation determined that an unauthorized party had accessed the email accounts of three Canto Rausch employees at various times between March 23, 2019 and August 15, 2019. Based on the investigation, some personal information of a New Hampshire resident was potentially accessible, including name, Social Security number, driver's license number, financial account information, payment card information, and other tax-related information.

On November 1, 2019, Canto Rausch will begin mailing written notifications to potentially affected individuals, including one New Hampshire resident who is being notified of the incident in writing in accordance with N.H. Rev. Stat. Ann. § 359-C:20 in substantially the same form as the enclosed letter.¹ Canto Rausch is offering a complimentary one year membership in credit monitoring and identity theft protection services through Kroll to the New Hampshire individual whose Social Security number or driver's license number was potentially contained in the email

¹ This report does not waive Canto Rausch's objection that New Hampshire lacks personal jurisdiction over this matter.

November 1, 2019

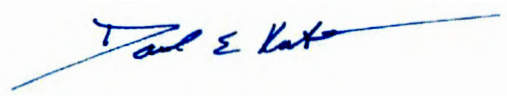
Page 2

accounts. Canto Rausch has also provided a telephone number for potentially affected individuals to call with any questions they may have.

To further protect personal information, Canto Rausch has taken steps to enhance its existing security and email protocols and to re-educate its staff to be on alert for these types of incidents.

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

Sincerely,

A handwritten signature in blue ink, appearing to read "David E. Kitchen", with a long horizontal flourish extending to the right.

David E. Kitchen
Partner

Enclosure

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

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

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

At Canto, Rausch, Deck & Co., P.A. ("Canto Rausch"), we recognize the importance of securing and protecting the personal information of our clients. Regrettably, we recently learned of an incident that may have involved some of your information. This letter explains the incident, measures we have taken, and some steps you can take in response.

Our investigation into an email phishing incident recently determined that an unauthorized individual may have gained access to a small number of employee email accounts. Upon first learning of the incident, we took immediate steps to secure all Canto Rausch email accounts. We also began an investigation with the assistance of a cybersecurity firm. The investigation determined that an unauthorized party had accessed the email accounts of three Canto Rausch employees at various times between March 23, 2019 and August 15, 2019.

For two of these accounts, the investigation was unable to determine which emails and attachments had been viewed by the unauthorized person. We are therefore providing notice to all clients who may have provided personal information to either of the affected email accounts. If you provided information to your CPA or his assistant by email, it may have included your name, Social Security number, driver's license number, bank account numbers, and other tax-related information. If you have dependent(s), you may have also supplied the same information pertaining to them.

To help protect your identity and as a precaution, we are offering complimentary identity monitoring for one year through Kroll. Kroll provides risk mitigation and response services, and their team is experienced in helping people who have sustained an unintentional exposure of confidential data. 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 **January 24, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

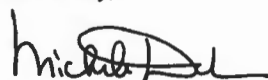
For additional information regarding the identity monitoring services being offered, please see the next section of this letter.

Please note that if you provided Canto Rausch with information for any dependent(s), we are also prepared to offer complimentary identity monitoring services for those individuals through Kroll. You may request these services for your dependents by calling the phone number provided below.

You should always remain vigilant for incidents of fraud or identity theft by reviewing your free credit reports for any unauthorized activity. Please see the pages that follow this notice for additional steps you may take to protect your information.

Your confidence and trust are important to us, and we regret any inconvenience or concern this may cause. To further protect personal information, we have taken steps to enhance our existing security and email protocols and to re-educate our staff to be on alert for these types of incidents. If you have any questions, please call 1-844-996-1024 Monday through Friday from 9:00 a. m. to 6:30 p.m. Eastern Time, excluding U.S. national holidays.

Sincerely,



Michele Deck
Managing Partner

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 can 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 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 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.

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:

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

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

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 in order to correct your records. Contact information for the Federal Trade Commission is as follows:

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

If you are a resident of Maryland or North Carolina, you may contact and obtain information from your state attorney general at:

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023 / (410) 576-6300 (for calls originating outside Maryland), www.oag.state.md.us

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, 919-716-6400 / 1-877-566-7226, www.ncdoj.gov

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

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.

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. Addresses at which you have lived over the past 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 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 wish to have the credit report available. The credit reporting agencies have one hour 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 hour 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.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance, or employment, if you ask for your report within 60 days of receiving notice of said action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.