BRIAN MIDDLEBROOK
PARTNER
BMIDDLEBROOK@GRSM.COM

GORDON&REES
SCULLY MANSUKHANI
YOUR 50 STATE PARTNER™

ATTORNEYS AT LAW
1 BATTERY PARK PLAZA, 28TH FLOOR
NEW YORK, NY 10004
WWW.GRSM.COM

March 30, 2020

VIA ELECTRONIC MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
Gordon J. MacDonald, Attorney General
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of Data Security Incident
Our File No: 1203248

Dear Attorney General MacDonald:

Our client, BCHH, Inc. ("BCHH"), a nationwide title solutions provider headquartered in Coraopolis, Pennsylvania which provides comprehensive title insurance products and escrow services, understands the importance of protecting the personal information provided by its customers and is making this notification to your Office in accordance with applicable law following a recent data security incident.

On October 15, 2019, following a period of limited suspicious activity, BCHH determined that one of its employee's email accounts may have been compromised. BCHH immediately requested that its IT consultant evaluate BCHH's workspace to identify any signs of unauthorized access to the network and Office365 ("O365") environment. The consultant determined that the employee's email account password was compromised and certain inbox rules were put in place. The consultant immediately changed all passwords associated with the employee's O365 account and took affirmative steps to further safeguard the integrity of the account, including a comprehensive scan, removal of all inbox rules and confirmation of termination of any potential unauthorized access.

BCHH and its IT consultant also undertook additional affirmative steps to ensure the security and integrity of its systems on an enterprise-wide basis, including changing all passwords associated with BCHH's O365 environment and implementation of multi-factor authentication. The consultant also undertook an investigation to identify any additional O365 accounts which may have been compromised. The investigation did not identify any signs of unauthorized access to any additional accounts beyond the one (1) account discussed above.

Following completion of the internal investigation and remediation efforts, BCHH undertook a comprehensive external forensic investigation to determine the complete nature of the

data security incident and identify any individuals whose personal information may have been compromised. The forensic investigation confirmed that only one (1) O365 account associated with BCHH was compromised. Because of the deliberate efforts of the malicious actor(s) and the limited historic information available, the forensic investigation was unable to determine an initial start date of the compromise or method of access, though it was confirmed that the threat was terminated on October 15, 2019, the same day that the compromise was identified.

As a result, to exhaust investigative efforts, a full and time-consuming analysis of the impacted mailbox was performed. The investigation identified the existence of personal information within this mailbox account, including social security numbers, individual taxpayer identification numbers, and drivers' license numbers. While it cannot be ruled out that the information was not accessed or acquired by the malicious actor, there is also no evidence that it was. The extensive analysis concluded on February 27, 2020.

In an abundance of caution, written notification will be provided to all potentially impacted individuals beginning March 27, 2020, including one (1) New Hampshire resident. A sample copy of the notification to the New Hampshire resident is attached. As noted in the attachment, BCHH has included an offer to provide twenty-four months of comprehensive identity monitoring services, including three-bureau credit monitoring, to the New Hampshire resident.

BCHH is and remains committed to protecting the integrity of personal information contained on its servers, and continues to work closely with security experts to identify and implement additional measures to further strengthen the security of its system to help prevent a similar event from happening in the future. As noted above, in addition to the security protocols already in place, following identification of the data security incident, BCHH took immediate affirmative steps to further safeguard the continued security and integrity of the impacted account and its systems on an enterprise-wide basis. Specifically, BCHH's IT consultant immediately changed all passwords associated with the impacted account, undertook a comprehensive scan, removed all inbox rules and confirmed termination of any potential unauthorized access. The consultant also changed all passwords associated with BCHH's O365 environment and implemented multi-factor authentication on an enterprise-wide basis.

Should you have any questions or require additional information, please do not hesitate to contact me.

Best regards,

GORDON REES SCULLY MANSUKHANI, LLP

/s/ Brian Middlebrook

Brian Middlebrook, Esq.

Enclosures

Nationwide. Full Service. Title Agency
BCHH
Our Name is Behind Our Service.

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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

BCHH, Inc. ("BCHH") values your business and understands the importance of safeguarding your personal information. We recently identified and addressed a security incident that potentially may have involved some of your personal information. This letter describes the incident, outlines the measures we have taken in response, and advises you of steps you can take to further protect your information.

What Happened?

On October 15, 2019, following a period of limited suspicious activity, BCHH determined that one of its employee's email accounts may have been compromised. BCHH immediately requested that its IT consultant evaluate BCHH's workspace to identify any signs of unauthorized access to the network and Office365 ("O365") environment. The consultant determined that the employee's email account password was compromised and certain inbox rules were put in place. The consultant immediately changed all passwords associated with the employee's O365 account and took affirmative steps to further safeguard the integrity of the account, including a comprehensive scan, removal of all inbox rules and confirmation of termination of any potential unauthorized access.

BCHH and its IT consultant also undertook additional affirmative steps to ensure the security and integrity of its systems on an enterprise-wide basis, including changing all passwords associated with BCHH's O365 environment and implementation of multi-factor authentication. The consultant also undertook an investigation to identify any additional O365 accounts which may have been compromised. The investigation did not identify any signs of unauthorized access to any additional accounts beyond the one (1) account discussed above.

What Information Was Involved?

Following completion of the internal investigation and remediation efforts, BCHH undertook a comprehensive external forensic investigation to determine the complete nature of the data security incident and identify any individuals whose personal information may have been compromised. The forensic investigation confirmed that only one (1) O365 account associated with BCHH was compromised. Because of the deliberate efforts of the malicious actor(s) and the limited historic information available, the forensic investigation was unable to determine an initial start date of the compromise or method of access, though it was confirmed that the threat was terminated on October 15, 2019, the same day that the compromise was identified.

As a result, to exhaust investigative efforts, a full and time-consuming analysis of the impacted mailbox was performed. The investigation identified the existence of personal information within this mailbox account, including Social Security numbers, individual taxpayer identification numbers, and drivers' license numbers. While it cannot be ruled out that the information was not accessed or acquired by the malicious actor, there is also no evidence that it was, which is why this notice is provided in an abundance of caution. The extensive analysis concluded on February 27, 2020. We are providing this notification to you as you are one of the individuals with personal information identified in the impacted mailbox. Please note that it is entirely possible that your specific personal information was not affected.

What We Are Doing

As noted above, in addition to the security protocols already in place, following identification of the data security incident, BCHH took immediate affirmative steps to further safeguard the continued security and integrity of the impacted account and its systems on an enterprise-wide basis. Specifically, BCHH's IT consultant immediately changed all passwords associated with the impacted account, undertook a comprehensive scan, removed all inbox rules and confirmed termination of any potential unauthorized access. The consultant also changed all passwords associated with BCHH's O365 environment and implemented multi-factor authentication on an enterprise-wide basis. BCHH is and remains committed to protecting the integrity of personal information contained on its servers, and continues to work closely with security experts to identify and implement additional measures to further strengthen the security of its system to help prevent a similar event from happening in the future.

In an additional showing of support for our valued clients, we have secured the services of Kroll to provide three-bureau identity monitoring at no cost to you for two years. 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, fraud consultation and identity theft restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **June 26, 2020** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

What You Can Do

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information

We value your past and on-going business and deeply regret any concerns this letter may cause to you. **Should you have any questions, please call 1-877-514-0832 between the hours of 8:00 a.m. and 5:30 p.m. Central Standard Time. Please have your membership number ready.** In the event the call-in center is unable to assist you, please do not hesitate to contact BCHH directly at (412) 249-8241.

Sincerely,

Charles Marino
President, BCHH, Inc.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability 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 may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. 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.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] 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'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 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.