Clark Hill

Jason M. Schwent
T (312) 985-5939
F (312) 517-7573
Email:jschwent@clarkhill.com

Clark Hill
130 E. Randolph Street Suite 3900
Chicago Illinois 60601
T (312) 985-5900
F (312) 985-5999

September 9, 2022

Via Electronic Mail

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
attorneygeneral@doj.nh.gov

Dear Attorney General Formella:

We represent Byron Cotton ("Mr. Cotton") with respect to a data security incident involving the potential exposure of certain personally identifiable information described in more detail below. Bryon Cotton is an attorney and owns a real estate title company located in Shalimar, Florida. Mr. Cotton is committed to answering any questions you have about this incident, his response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On March 3, 2022, Mr. Cotton learned of suspicious activity associated with his corporate email account. As soon as Mr. Cotton learned of this activity, he began an internal investigation and hired a third-party vendor to conduct an in-depth review of the email account to determine whether there was any unauthorized access to the affected email account, what personal information may have been located in the account, and to extract contact information of potentially affected individuals. The investigation found, on April 18, 2022, that there had been unauthorized access to the account in question, but could not determine what the unauthorized actor had done within the account. Mr. Cotton hired an independent vendor to review the contents of the entire email account to determine what personal information may have been within the account. This review was completed on August 21, 2022. That review found that some limited personal information for individuals may have been located in the corporate email account at issue. While Mr. Cotton has no indication that any personal information was compromised or misused as a result of this incident, out of an abundance of caution, he is notifying individuals of this incident. Information that was located in the corporate email account includes names, addresses, and some combination of the following: Social Security numbers, dates of birth, driver's license information, limited financial account information, and health insurance or medical treatment information.

2. Number of residents affected.

One (1) New Hampshire resident may have been affected and was notified of the incident. A notification letter was sent to the potentially affected individual on September 9, 2022 (a copy of the form notification letter is enclosed as Exhibit A).

3. Steps taken in response to the incident.

Mr. Cotton has taken steps to enhance the security of his systems. The password to the affected corporate email account was changed and multifactor authentication was enabled across all corporate email accounts. Additionally, individuals were offered 12 months of credit monitoring and identity protection services through Cyberscout where available.

4. Contact information.

Mr. Cotton takes the security of the information in his control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

Jason M. Schwent
Senior Counsel

cc: Mariah Leffingwell – mleffingwell@clarkhill.com

Cotton Land Title, LLC
P.O. Box 3923
Syracuse, NY 13220

«First_Name» «Middle_NameInitial» «Last_Name»
«Address_1»
«Address_2_»
«City», «State» «Zip»

September 9, 2022

«Title»

Dear «First_Name» «Last_Name»,

I recently experienced a data security incident that may have impacted some of your personal information. I take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources I am making available to help you.

What happened?

On March 3, 2022, I learned of suspicious activity associated with my corporate email account. As soon as I learned of this activity, I began an internal investigation and hired a third-party vendor to conduct an in-depth review of the email account to determine whether there was any unauthorized access to the affected email account, what personal information may have been located in the account, and to extract contact information of potentially affected individuals. The investigation found, on April 18, 2022, that there had been unauthorized access to the account in question, but could not determine what the unauthorized actor had done within the account. I hired an independent vendor to review the contents of the entire account and what personal information may have been within the account and completed that review on August 21, 2022. That review found that some of your personal information may have been located in the corporate email account at issue. While I have no indication that any of your personal information was compromised or misused as a result of this incident, out of an abundance of caution, I wanted to notify you about this incident and provide you with resources to protect yourself.

What information was impacted?

From the review, it appears that your name, «Variable_Text_1» may have been impacted by this incident.

What I am doing:

I want to assure you that I have taken steps to prevent this kind of event from happening in the future. Since the incident, the password to the affected corporate email account was changed and multifactor authentication was enabled across all corporate email accounts.

What you can do:

It is always a good idea to remain vigilant for incident of identity theft or fraud, and to review your bank account and other financial statements as well as your credit reports for suspicious activity. I also encourage you to contact Cyberscout with any questions. Additional information about protecting your identity is included in this letter, 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:

If you have any questions or concerns, please call **1-800-405-6108** Monday through Friday from 8:00 am to 8:00 pm Eastern Time. Your trust is our top priority, and I deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Byron Cotton
Cotton Land Title, LLC

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

1. We recommend you review your credit reports. 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 reporting companies. 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.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert 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 bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

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

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. 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 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. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There are [0] Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft