

Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email: mventrone@ClarkHill.com

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

September 18, 2023

Via Electronic Mail

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

We represent John P. Gallina Law Offices with respect to a data security incident described in more detail below. John P. Gallina Law Offices is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident

On April 25, 2023, John P. Gallina Law Offices became aware of suspicious activity associated with an email account, and immediately began an investigation to determine what occurred and whether any information was at risk. The investigation determined that there was unauthorized access to one email account for a limited period of time, although the investigation was unable to determine whether any information was accessed or acquired. John P. Gallina Law Offices engaged an independent computer forensic firm to review the information in the account to identify and extract any personal identifiable information. This process was completed on July 25, 2023, at which point John P. Gallina Law Offices identified those individuals whose personal information was present in the account. Information that may have been impacted includes names, addresses, and some combination of the following: driver's license numbers, Social Security numbers, bank account information, and financial account information.

2. Number of residents affected

Three (3) Maryland residents may have been affected and was notified of the incident. A notification letter was sent to the potentially affected individuals on September 19, 2023 via regular mail (a copy of the form notification letter is enclosed).

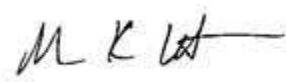
3. Steps taken in response to the incident

In response to this incident, the password for the corporate email account was reset and John P. Gallina Law Offices implemented additional restrictions on providing or receiving personal information by email, and improved their security posture by conducting additional malware and virus scans of the corporate email account. In addition, they have arranged for affected individuals to receive credit monitoring and identity protection services provided by TransUnion.

4. Contact information

John P. Gallina Law Offices takes the security of the information in its control seriously and is committed to ensuring the information in its control is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,
CLARK HILL

A handwritten signature in black ink, appearing to read 'M K Ventrone', with a horizontal line extending to the right.

Melissa K. Ventrone
Member

CC: Paul Schmeltzer

John P. Gallina Law Offices
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07920 1-1



September 19, 2023

Notice of Data Security Incident

[REDACTED],

We are writing to inform you of a recent data security incident experienced by John P. Gallina Law Offices that may have impacted your personal information described in more detail below. We 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 we are making available to help you.

What Happened?

On April 25, 2023, we learned that there had been unauthorized access to one of our email accounts. We conducted an investigation to determine whether any personal information was at risk, but were unable to determine whether any emails or documents were viewed or taken during the period of unauthorized access. Out of an abundance of caution, we engaged a vendor to review the emails and documents contained in the email account to identify any personal information. This process was completed on July 25, 2023, at which point we determined that your information may have been present during the period of unauthorized access.

What Information Was Involved?

Impacted information may include some combination of your Social Security number.

What we are doing:

We have taken steps to prevent a similar incident in the future, including changing the password for the email account, implementing additional restrictions on providing or receiving personal information by email, and improving our security posture by conducting additional malware and virus scans of the email account.

Although we have no evidence your information has been misused, we arranged for you to receive Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below.

For more information:

If you have any questions or concerns, please contact 1-800-405-6108. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when enrolling, so please do not discard this letter. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

John P. Gallina

Recommended Steps to help Protect your Information

1. Website and Enrollment. To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/jpgesq> and follow the instructions provided. When prompted please provide the following unique code to receive services: 4QX9LH8TK8 In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

2. Activate the credit monitoring provided as part of your services with Cyberscout. The monitoring included must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, Cyberscout will be able to provide guidance.

3. Telephone. Contact Cyberscout at 1-800-405-6108 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring 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.

If you discover any suspicious items and have enrolled in Cyberscout credit monitoring, notify them immediately by calling 1-800-405-6108 from 8:00 am to 8:00 pm Eastern, Monday through Friday.

A representative will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be able to work with a representative who will assist you with resolving any fraudulent activity.

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.

5. 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
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.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

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.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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/201504_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. A total of 1 Rhode Island residents were notified of this incident.

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