

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

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

March 4, 2024

***VIA ELECTRONIC MAIL***

Office of the Attorney General  
Identity Theft Unit  
200 St. Paul Place  
Baltimore, MD 21202  
[IDTheft@oag.state.md.us](mailto:IDTheft@oag.state.md.us)

Dear Attorney General Brown:

We represent the Law Office of Daniel Shapiro (“Shapiro”) with respect to a data security incident involving the potential exposure of certain personally identifiable information (“PII”) described in more detail below. Shapiro, a law firm located in Montclair, NJ, is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident from occurring in the future.

**1. Nature of security incident.**

On November 27, 2023, Shapiro was alerted to a misdirected wire transfer associated with one of their clients. They immediately started an internal investigation and hired an independent computer forensics firm to help with the investigation. On January 2, 2024, the investigation found unauthorized access to one email account but was unable to determine what specific information within the account had actually been accessed. Out of an abundance of caution, Shapiro hired a vendor to do an in-depth review of the account to determine what personal information may have been present during the period of unauthorized access. This review was completed on February 1, 2024. From this review, it appears the information in the account may have included individual’s names, and some combination of the following data elements: address, date of birth, Social Security number, financial account information, state and government ID numbers, payment card information, health insurance information, and limited medical information.

**2. Number of residents affected.**

One (1) Maryland resident may have been affected and was notified of the incident. A notification letter was sent to the potentially affected individual on March 4, 2024. A copy of the form notification letter is enclosed.

March 4, 2024

Page 2

**3. Steps taken in response.**

Since this incident, Shapiro changed the password to the affected email account and multifactor authentication was enabled for remote access to Shapiro email accounts. Additionally, impacted individuals were offered 12 months of credit monitoring and identity protection services through Cyberscout.

**4. Contact information.**

Shapiro takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at [jschwent@clarkhill.com](mailto:jschwent@clarkhill.com) or (312) 985-5900.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read 'JS', followed by a horizontal line.

Jason M. Schwent

The Law Office of Daniel B. Shapiro  
c/o Cyberscout  
1 Keystone Ave., Unit 700  
Cherry Hill, NJ 08003  
DB-08577

LAW OFFICE OF  
**DANIEL B. SHAPIRO**

March 4, 2024

## **Notice of Data Security Incident**

Dear 

The Law Office of Daniel Shapiro is writing to let you know about a data security incident that may have affected your personal information. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this incident may cause you. This letter contains information about what occurred, steps you can take to protect your information, and resources we are making available to help you do so.

### **What happened?**

On November 27, 2023, we were alerted to a misdirected wire transfer associated with one of our clients. We immediately started an internal investigation and hired an independent computer forensics firm to help with our investigation. On January 2, 2024, the investigation found unauthorized access to one email account but was unable to determine if any information in the account was accessed. Out of an abundance of caution, we hired a vendor to do an in-depth review of the account to determine what personal information may have been present during the period of unauthorized access. This review was completed on February 1, 2024, at which point we identified that some of your personal information may have been located in the account during the period of unauthorized access.

We want to emphasize that we have no evidence that your personal information was compromised or misused. Out of an abundance of caution, we 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, address, Social Security number, financial information, and financial account number may have been impacted by this incident.

### **What we are doing:**

We want to assure you that we have taken steps to prevent this kind of event from happening in the future. Since the incident, the passwords to the affected email account were changed and multifactor authentication was enabled across all Law Office of Daniel Shapiro email accounts.

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 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.

**How do I enroll for the free services?**

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/lawofficeofdbshapiro> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

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.

**What you can do:**

It is always a good idea to remain vigilant and be on the look-out for evidence of identity theft or fraud, and to review your bank account and other financial statements as well as your credit reports for suspicious activity. We also encourage you to contact Cyberscout with any questions and to take full advantage of the Cyberscout service offering. 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, 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 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed above. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

*The Law Office of Daniel Shapiro*

## RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

*You've been provided with access to the following services from Cyberscout:*

**1. 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 Cyberscout fraud specialist, who can help you determine if it's an indicator of identity theft.

**2. Fraud Consultation.** You have unlimited access to consultation with a Cyberscout 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.

**3. Identity Theft Restoration.** If you become a victim of identity theft, an experienced Cyberscout 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.

**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](http://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 IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who 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 assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://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](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

**District of Columbia Residents:** Office of the Attorney General, 400 6<sup>th</sup> Street, NW, Washington, DC 20001; 202-727-3400; [oag@dc.gov](mailto:oag@dc.gov).

**Iowa Residents:** Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; [consumer@ag.iowa.gov](mailto:consumer@ag.iowa.gov).

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://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](http://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](http://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](http://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/](http://www.doj.state.or.us/), Telephone: 1-877-877-9392.

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 1-401-274-4400. Total Rhode Island residents notified is 0.

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