



Jason Cherry  
633 West 5<sup>th</sup> Street, Suite 4000  
Los Angeles, CA 90071  
Jason.Cherry@lewisbrisbois.com  
Direct: 213.358.6067

June 3, 2022

**VIA ELECTRONIC MAIL**

Attorney General Brian Frosh  
Maryland Attorney General's Office  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
E-Mail: Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

We represent Shapiro & Duncan, Inc. ("Shapiro & Duncan"), a construction and engineering company based in Rockville, Maryland, in connection with a recent data security incident described in greater detail below.

**1. Nature of the security incident.**

On February 17, 2022, Shapiro & Duncan detected unusual activity in its network environment. Upon discovering this activity, Shapiro & Duncan took immediate steps to secure its network and launched an investigation with the assistance of outside cybersecurity experts to determine what happened and whether sensitive information was accessed or acquired without authorization. As a result of this investigation, Shapiro & Duncan learned that certain network systems had been accessed without authorization, including certain systems that stored personal information of its employees. Shapiro & Duncan promptly reviewed these systems to identify the individuals to whom the information pertained and worked diligently to obtain up-to-date address information in anticipation of providing notification. Shapiro & Duncan concluded that process on May 4, 2022 and promptly arranged for impacted individuals to be notified.

The information that may have been accessible by the malicious actor(s) responsible for this incident includes Social Security number, financial account number, health insurance identification number, and medical treatment information.

**2. Number of Maryland residents affected.**

Shapiro & Duncan will notify One thousand two hundred and nine (1,209) Maryland residents via the attached sample letter, or a substantially similar version, on June 3, 2022.

### **3. Steps taken relating to the Incident.**

As soon as Shapiro & Duncan discovered this incident, Shapiro & Duncan took steps to secure its network environment and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. Shapiro & Duncan has also implemented additional safeguards to help ensure the security of its environment and reduce the risk of a similar incident occurring in the future, including enhancing its cybersecurity awareness training program for employees and implementing additional safeguards within its email environment. Shapiro & Duncan also reported this incident to the Federal Bureau of Investigation and will provide any assistance necessary to help hold the perpetrator(s) accountable.

Shapiro & Duncan has also established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. In addition, while Shapiro & Duncan is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Shapiro & Duncan is also providing complimentary identity protection services to notified individuals.

### **4. Contact information.**

Shapiro & Duncan is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please contact me at [Jason.Cherry@lewisbrisbois.com](mailto:Jason.Cherry@lewisbrisbois.com) or David McMillan at [David.McMillan@lewisbrisbois.com](mailto:David.McMillan@lewisbrisbois.com).

Sincerely,

A handwritten signature in blue ink that reads "Jason S. Cherry". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

Jason Cherry of  
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Consumer Notification Letter



Return to IDX:  
10300 SW Greenburg Rd.  
Suite 570  
Portland OR, 97223

To Enroll, Please Call:  
(833) 903-3648  
Or Visit:  
<https://app.idx.us/account-creation/protect>  
Enrollment Code:  
<<enrollment code>>

<<First Name>> <<Last Name>>  
<<Address1>> <<Address2>>  
<<City>>, <<State>> <<Zip>>

June 3, 2022

**Re: Notice of Data Security Incident**

Dear <<First Name>> <<Last Name>>,

We are writing to notify you that Shapiro & Duncan recently experienced a data security incident that may have involved your personal information. Shapiro & Duncan is committed to maintaining your trust and demonstrating our commitment to the privacy and security of all information in our possession. That is why we are contacting you to notify you that this incident occurred and to offer you complimentary credit monitoring and identity theft restoration services. We are also providing you with information, included at the end of this letter, about steps you can take on your own to help safeguard your personal information. We encourage you to read this information carefully.

**What Happened.** On February 17, 2022, we discovered a data security incident that disrupted access to certain Shapiro & Duncan network systems. Within a few hours, we had launched an investigation with the assistance of a leading digital forensics and incident response firm to help us determine what happened and whether any Shapiro & Duncan information may have been impacted. Based on the investigation, we determined that Shapiro & Duncan had been victimized by a sophisticated cyber incident that affected certain systems, some of which stored your personal information. We immediately began to review these systems in order to determine precisely what information may have been involved and identify the individuals who may have been impacted. We then worked diligently to gather up-to-date contact information for impacted individuals for purposes of providing notification. We completed that process on May 4, 2022, and promptly arranged for this letter to be sent.

**What Information Was Involved.** The information involved may include your name, Social Security number, financial account number, health insurance identification number, and medical treatment information.

**What We Are Doing.** As soon as we discovered the incident, we launched an investigation and took steps to secure our network, including by implementing enhanced security measures to prevent a similar incident from happening again. We also reported the incident to the Federal Bureau of Investigation, and will provide whatever assistance is necessary to help hold the perpetrators accountable. Furthermore, out of an abundance of caution we are offering you << length of monitoring >> of complimentary credit monitoring and identity protection services through IDX, a data security and recovery services expert. Your complimentary IDX identity monitoring and protection services include: credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. Additional information about these services is included with this letter. To take advantage of these services, you must follow the instructions in this letter to enroll. We are also providing you with the information below about steps you can take on your own to help protect your personal information.

**What You Can Do.** We strongly encourage you to enroll in the credit monitoring and identity monitoring services we are offering through IDX using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is September 3, 2022. We also encourage you to closely review the recommendations included with this letter to help protect your personal information.

**For More Information.** You will find detailed instructions for enrollment on the enclosed document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call (833) 903-3648 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. Thank you for your patience and understanding. We take your trust in us and this matter very seriously.

Sincerely,

A handwritten signature in dark ink, appearing to read "Charles P. Ayres". The signature is fluid and cursive, with the first name "Charles" being the most prominent part.

Charles P. Ayres  
Chief Operating Officer  
Shapiro & Duncan, Inc.

## Steps You Can Take to Protect Your Personal Information

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

**Equifax**

P.O. Box 105851  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

**Experian**

P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-916-8800  
[www.transunion.com](http://www.transunion.com)

**Fraud Alert:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

**Security Freeze:** You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

**Federal Trade Commission**

600 Pennsylvania Ave, NW  
Washington, DC 20580  
[consumer.ftc.gov](http://consumer.ftc.gov), and  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

**Maryland Attorney General**

200 St. Paul Place  
Baltimore, MD 21202  
[oag.state.md.us](http://oag.state.md.us)  
1-888-743-0023

**New York Attorney General**

Bureau of Internet and Technology  
Resources  
28 Liberty Street  
New York, NY 10005  
1-212-416-8433

**North Carolina Attorney General**

9001 Mail Service Center  
Raleigh, NC 27699  
[ncdoj.gov](http://ncdoj.gov)  
1-877-566-7226

**Rhode Island Attorney General**

150 South Main Street  
Providence, RI 02903  
<http://www.riag.ri.gov>  
1-401-274-4400

**Washington D.C. Attorney General**

441 4th Street, NW  
Washington, DC 20001  
[oag.dc.gov](http://oag.dc.gov)  
1-202-727-3400

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



## IDX Identity Protection Services

**Website and Enrollment.** Please visit <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code included with this letter.

**Activate the credit monitoring** provided as part of your membership. The monitoring included in the membership 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, IDX will be able to assist you.

**Telephone.** Contact IDX at (833) 903-3648 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**IDX Identity will include <<monitoring length>> of enrollment into the following service components:**

**SINGLE BUREAU CREDIT MONITORING** - Monitoring of credit bureau for changes to the member's credit file such as new credit inquiries, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

**CYBERSCANTM** - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, and phone numbers.

**IDENTITY THEFT INSURANCE** - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

**FULLY-MANAGED IDENTITY RECOVERY** – IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned ID Care Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.